Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance

Schermer, B.W.

Software agents, surveillance, and the right to privacy:
a legislative framework for agent-enabled surveillance

Leiden University Press

SIKS dissertation series no. 2007-05
The research reported in this thesis has been carried out under the auspices of SIKS, the Dutch Research School for Information and Knowledge Systems

Lay-out: Anne-Marie Krens – Tekstbeeld – Oegstgeest

Leiden University Press is an imprint of Amsterdam University Press

ISBN 978 90 8728 021 5

Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance

PROEFSCHRIFT

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van de Rector Magnificus prof. mr. P.F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 9 mei 2007
klokke 15.00 uur

door

Bart Willem Schermer

geboren te Alkmaar in 1978

Promotiecommissie:

Promotor:	Prof. dr. H.J. van den Herik
Referent:	Prof. dr. H. Franken
Overige leden:	Prof. dr. F.M.T. Brazier (Vrije Universiteit Amsterdam)
	Prof. dr. R.E. van Esch
	Prof. dr. E.O. Postma (Universiteit Maastricht)
	Prof. dr. A.H.J. Schmidt
	Prof. mr. J.L. de Wijkerslooth

Preface

To write this thesis I used an Apple laptop computer that gave me access to a variety of cognitive tools such as a word processor, a PDF reader, and the internet. A mere twenty years ago I would not have had the benefit of these technologies, either because they did not exist, or because they were not yet ready for mass adoption. To me this illustrates how fast technology is changing our lives.

The pace at which technology is developing accelerates at an exponential rate (Kurzweil 2005). Between the development of agriculture in the Fertile Crescent and the invention of the wheel lies a period of four thousand years. Between the invention of the catapult and the invention of the cannon there is a period of two thousand years, and the period between the development of paper and the movable type printing press is a thousand years. The invention and mass adoption of technologies such as cars, airplanes, computers, and the internet all took place in the past century.

I believe that the accelerated development and the current convergence of new technologies will greatly benefit mankind. For instance, future technologies will have the potential to stop the environmental damage that threatens our planet, help to eliminate poverty, and will successfully combat the effects of old age. However, while the potential benefits of technology are considerable, the risks that flow forth from misuse and abuse are also substantial.

My primary motivation for writing this thesis is as follows: I feel that we have reached a point in time where the pace of technological development is so fast, and its potential impact on society so significant, that the introduction and subsequent use of disruptive future technologies should be subjected to a closer scrutiny than so far takes place. In my opinion society as a whole should become more aware of the policy issues surrounding new technologies.

For this thesis I have chosen to focus on specific policy issues related to artificial intelligence technology. In the summer of 1956 the Dartmouth College hosted the first conference on artificial intelligence. Now, fifty years later, the use of artificial intelligence is widespread within our society, despite the fact that artificial intelligence acting on the level of a human being has not yet been achieved.

One area in particular that can benefit from the application of artificial intelligence is surveillance. Using artificial intelligence technology for sur-

veillance purposes can increase national security and public safety. However, this also places additional power into the hands of the government. It is therefore important to give careful consideration to the ways in which governments use surveillance technologies, and how these technologies may change the balance of power within society.

The great statesman and third president of the United States, Thomas Jefferson, once said: "the price of freedom is eternal vigilance". In this time of high technology I feel Jefferson's statement is even more relevant. The power of technology can quickly distort the balance of power between the populace and their elected leaders, or may have other unwanted or unintended consequences. Therefore, it is essential to remain vigilant when it comes to the use of powerful new technologies for surveillance purposes. By keeping a close eye on the use of new technologies we may ensure that we reap their benefits, while avoiding possible negative effects. I hope that by writing this thesis I will have contributed to this goal.

Bart W. Schermer
Leiden, January 2007

Table of Contents

Abbreviations

ACL	Agent Communication Language
ACLU	American Civil Liberties Union
AI	Artificial Intelligence
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AmI	Ambient Intelligence
ANITA	Administrative Normative Information Transaction Agents
BDI	Belief, Desire, Intention
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CCP	Dutch Code of Criminal Procedure
CCTV	Closed Circuit Television
CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Projects Agency
DDM	Distributed Data Mining
DOJ	Department of Justice
GAO	Government Accountability Office
EC	European Commission
ECHR	European Court of Human Rights / European Convention on Human Rights
EELD	Electronic Evidence and Link Discovery
FBI	Federal Bureau of Investigation
FIPA	Foundation for Intelligent Physical Agents
FISA	Foreign Intelligence Surveillance Act of 1978
FOIA	Freedom of Information Act
GPS	Global Positioning System
ICCPR	International Covenant on Civil Rights and Political Rights
ICT	Information and Communication Technology
IPv6	Internet Protocol Version 6
IRC	Internet Relay Chat
KDD	Knowledge Discovery in Databases
KQML	Knowledge Query Manipulation Language
MAS	Multi-Agent System
MID	Militaire Inlichtingen Dienst
MOUT	Military Operations in Urban Terrain
NCCUSL	National Conference of Commissioners on Uniform State Laws
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
PDF	Portable Document Format
PETs	Privacy Enhancing Technologies

PFA	Police Files Act
RFID	Radio Frequency Identification
TIA(O)	Total Information Awareness (Office)
TSP	Terrorist Surveillance Program
UDHR	Universal Declaration of Human Rights
UETA	Uniform Electronic Transactions Act
USC	United States Code
WIV	Wet op de Inlichtingen en Veiligheidsdiensten

1 Introduction

Human knowledge and human power meet in one,
For where the cause is not known the effect cannot be produced.
Francis Bacon

This thesis deals with the use of software agents as tools for surveillance. In particular, it studies the effects that agent-enabled surveillance might have on (individual) liberty and on the right to privacy. The issue to be investigated is twofold: (1) the ability of technology to facilitate social control through surveillance, and (2) the way in which we can ensure that surveillance techniques will be used in a responsible manner.

Sections 1.1 and 1.2 will set the stage for the thesis by providing a brief overview of general thoughts on surveillance, agents, liberty, privacy, and control. In section 1.3 I shall introduce computer science and investigate the software agent paradigm. Surveillance and control is the subject of section 1.4, where emphasis will be placed on electronic surveillance as a means to facilitate control. Section 1.5 will focus on the two related concepts privacy and liberty, special attention will be given to the ways in which software agents could jeopardise them. From there I shall continue on the road of surveillance and formulate in section 1.6 the problem definition to be discussed in the thesis. In section 1.7 I shall give a description of the research goal and in section 1.8 of the research approach. This chapter will be concluded with an outline of the thesis.

1.1 Knowledge is power

After the September 11 terrorist attacks, many western governments – most notably that of the United States – investigated ways to improve national security. Among the measures implemented by the United States government we see the passage of the USA Patriot Act and the foundation of the Total Information Awareness Office (TIA), which was later renamed to the less

ominously sounding (Terrorist) Information Awareness Office,[1,2] Both the Patriot Act and the TIA were aimed at improving the information position of the American intelligence community.

The inability of the intelligence community and other government agencies to predict and prevent the terrorist attacks made it clear that the American intelligence infrastructure was unable to cope with terrorism as a form of low-intensity/low-density warfare. The main problem was that different agencies involved in detecting the information signatures that terrorists usually leave behind, were unable to recognise, collect, and share the available information effectively. Moreover, none of the actors involved were able to 'connect the dots', in other words, derive a relevant meaning from distributed, heterogeneous information sources which, when connected, might have led to the discovery of the terrorists' plans. New and improved ways of identifying, collecting, and sharing information would therefore be needed to combat terrorism.

The idea that information plays a key role in fighting terrorism (or any other form of unacceptable human conduct) stems from the Baconian idea that 'knowledge is power' (Bacon 1597). In the *Novum Organum*, the second part of his never completed opus magnum the *Magna Instauratio*, Bacon (1561-1626) stated that human knowledge and human power meet in one (Bacon 1620). He argued that through knowledge mankind could assure its mastery over nature. But to attain knowledge on any given subject, a new system of *"true and perfect induction"* would be needed. The new system would replace the old scholastic system of scientific inquiry, which was based upon the Aristotelian tradition and religious dogma. Bacon's ideas on scientific method and intellectual reform played a key role in the birth of modern science.

Knowledge on a given subject enhances our understanding. This understanding can be used to exercise some form of power more effectively. Therefore knowledge is power. Whereas Bacon applied his adage to mankind's rule over nature, it could be argued that it is equally applicable to man's ability to rule his peers. The more we know about a group or an individual, the better our position for more effectively managing and influencing the group or the individual.

Modern society, with its widespread use of information and communication technology (ICT), provides unprecedented possibilities to obtain data from a variety of sources, so it seems that Bacon's aphorism is especially relevant within our networked 'information society'.[3]

---

1 USA Patriot Act of 2001, H.R. 3162, '*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*'

2 The Terrorist Information Awareness Office was discontinued when funding was repealed in September 2003 (Conference Report on H.R. 2658, Department of Defense Appropriations Act 2004, House Report 108-283).

3 Though the notion of ICT is almost exclusively used in the Netherlands, I prefer the abbreviation ICT over IT.

1.2 TECHNOLOGY AND CONTROL

Throughout the ages philosophers, from Plato to Habermas, have questioned the role of science and technology in society. Among these philosophers Heidegger is one of the foremost. Heidegger (1953) claimed that technology is relentlessly overtaking us. According to Heidegger, the essence of technology is the methodical planning of the future. This is clearly manifested in the exercise of human power over its surroundings. Heidegger reckoned that a new type of cultural system would emerge from this methodical planning which would restructure the entire world as an object of control (Feenberg 2000). Since humanity is unable to comprehend the essence of technology it has no real control over it (Heidegger 2002, p. 51). A recent advance in computer science, dubbed (software) agent technology, sheds new light on this argument.[4]

Agent technology is part of the science of artificial intelligence. An agent according to the Concise Oxford English Dictionary is: '*one who or that which exerts power or produces an effect*' (Soans and Stevenson, 2004). We all use agents in our daily life for a variety of tasks ranging from the mundane and boring ones to the highly complex ones. Examples of human agents include booking agents, secretaries, lawyers, and butlers. The agent concept can be interpreted to include software environments. Computer programs can be used to carry out tasks that have been delegated to them by a human user and act in this respect as an agent, albeit not a human one. They are therefore commonly called software agents, or intelligent agents. By using software agents, we relinquish part of the direct control we have and substitute it with indirect control through the agent.

Popular culture has taken up the software agent concept and expanded it into the realms of science fiction. The textbook example of an intelligent software agent that is in total control of its surroundings is HAL, the artificial-intelligence construct from the movie *2001: a Space Odyssey*.[5] As the ship's omniscient and omnipotent computer, HAL has full control over a spaceship heading for Jupiter. Just how far HAL's control reaches, is dramatically demonstrated when it turns against its human masters. Though HAL is a very good example of a software agent, there is an even better one: agent Smith from the movie *The Matrix*.[6] Agent Smith is the epitome of an intelligent software agent. Agent Smith is a software program that operates in a virtual environment known as the Matrix. To make matters a bit more complicated his function within the Matrix is also that of an agent. He looks and acts like a secret service agent and his task is to apprehend dissidents threatening the functioning of the Matrix. The power Agent Smith can wield as an agent is

4 From here on I shall use the term 'agent technology' instead of 'software agent technology'.
5 Warner Brothers, 1968.
6 Warner Brothers, 1999.

almost unlimited, in the Matrix he can even bend the laws of physics to accomplish his tasks.

In these dystopian visions of the future, humanity has lost control over its tools and sees its very existence threatened by the technology it created itself. While it is highly unlikely that such scenarios will ever become reality, the fact that software agents can act autonomously will have a significant impact on surveillance, privacy, and liberty. Whatever the future may hold, it seems likely that the agent paradigm will fundamentally alter the way in which we interact with computers in the years to come. Although this is probably a good thing, we must also take into account that agent technology will definitely raise certain ethical, moral, and legal issues, which need to be addressed now or in the near future. In this thesis I will try and solve one piece of the intricate agent puzzle.

1.3 Agents and interfaces

There is neither a single definition of a software agent, nor a set of attributes agreed upon for software agents. Instead 'software agent' is a kind of an umbrella term for software programs that display to some extent attributes commonly associated with agency (Nwana 1996, p. 2). This includes attributes such as autonomy, authority, and reactivity. In software environments agents are mostly used for: (1) solving the technical problems of distributed computing, and (2) overcoming the limitations of user interface approaches (Bradshaw 1998, p. 12-14).

The technical problems of distributed computing include amongst others: scalability, communication overhead, and load balancing. Agents can be used to overcome these problems by providing an intelligent approach to system interoperability (Bradshaw 1998, p. 12). Though the application of these types of agents could certainly raise some interesting legal issues, I shall not discuss the use of agents for distributed computing in this thesis. From the perspective of social control it is more interesting to look at the application of agents used to overcome the limitations of user interface approaches, since they can be used to facilitate control most effectively.

When we view the user interface as the link between man and machine, we can see that this link has evolved over time from a command-line interface to an object-driven, graphical user-interface. A command-line interface is a machine-centric interface. Users need to type in commands in a language the machine understands, in order to make the machine do what they want, which is a cumbersome, complex, user-unfriendly way of interaction. A graphical user interface is a more human-centric interface, since the way to manipulate the machine has been derived from the physical world. In a graphical user interface the interaction feels more like interacting with real-world objects. A human-centric approach thus makes interacting with the interface more

intuitive and efficient. The metaphor, in general, is fairly straightforward: the user sits behind a virtual desktop, files are stored in virtual folders, and when the user does not need them any longer, he can put them in a virtual wastebasket. In this way a user manipulates the computer environment by directly interacting with the objects on screen.[7] Graphical user interfaces are a powerful way of interacting with computers, but do have drawbacks that become apparent when the scale and/or complexity of the computing environment and the task at hand increase. The two main drawbacks of a graphical user interface are (1) the limitations of direct manipulation and (2) limited room for indirect management (Bradshaw 1998, p. 14-15). Loss of effective control is a direct result of these two drawbacks; therefore software agents are employed to regain control.

The limitations of direct manipulation

The first drawback of the graphical user interface is the need for direct manipulation of the computer. Though the graphical user interface is an improvement over the command-line interface in terms of speed and user friendliness, its design is still based on direct manipulation by a human user. Negroponte (1995, p. 99) argues that the future of human-computer interaction is not in direct manipulation via a user interface, but in delegation of tasks to a trusted system such as a software agent. Although most designers of graphical user interfaces centre on ease-of-use, they overlook the fact that interacting with a machine is still a means to accomplish a certain task, not an end in itself. Although an easy-to-use interface is certainly a benefit, it would be preferable to limit the need for interaction with a computer to a minimum. In the (near) future software agents will take over the tasks normally executed by humans, because these tasks are considered to be too tedious or repetitive, or because they are too complicated to be effectively executed via a direct manipulation user interface.

Limited room for indirect management

The second drawback of a graphical user interface, limited room for indirect management, ties in closely with the limits of direct manipulation. The solution proposed by Negroponte to overcome the limitations of direct manipulation lies in delegating tasks to the machine. This requires some form of indirect management. Current user interfaces leave little room for indirect management. What I mean by indirect management can be illustrated by an example from military history.

At the end of the First World War the German army adopted an indirect management style of command, called 'Auftragstaktik' (mission command), that hugely improved the combat efficiency of their units (Wawro 2000, p. 31).

---

7 For the sake of brevity I will use in this thesis only the male gender of nouns and pronouns in all cases where the person referred to could be either male of female.

Instead of designating an objective and the actions to be performed in order to achieve the objective (direct manipulation), central command decided to trust on the skills of their individual commanders in the field. The commander in the field had superior situational awareness and would only be hampered by centralised commands that curtailed his ability to act according to the needs of a continuously changing battlefield. So, in this new style of decentralised command, only the objective and some general guidelines were designated, but the actual planning and execution of the operation was left to the commander in field. Auftragstaktik, or indirect management, can also be implemented in a computer environment through the use of agent technology.

If a software agent is to function autonomously in a given environment, it needs to have an understanding of its surroundings, much like a field commander. Providing software agents with a sense of their surroundings and the ability to react to changes in their environment is one of the great challenges of artificial-intelligence research. To this end different agent architectures and multi-agent systems are being developed that enable agents to operate effectively in a given environment thus providing room for indirect management.

In a system that provides room for indirect management, a user could set forth a goal and not be involved in the actual execution of the task. Analogously to a field commander, an intelligent piece of software is oftentimes better suited to take decisions on how to execute a certain task than the user himself. Apart from this increase in efficiency, it also reduces the workload of the user.

Many different types of agents and agent systems are currently being developed and used to combat the drawbacks of user-interface approaches. One of the reasons for designing and building software agents is a growing demand for surveillance, which brings us to the subject of control.

1.4 Control and the surveillance society

Industrialisation and later on information and communication technology have led to significant changes in society. Franken (2004) has defined six characteristics of what is now fashionably called the 'Information society', they are: *dematerialisation, globalisation, turbulence, horizontalisation, vulnerability,* and *transparency*. The Dutch Commission on Civil Rights in the Digital Era[8] used these characteristics as a framework to define the policy issues related to the information society (Franken *et al.* 2000, p. 25). Below I give a brief description of these features, since they play an important role in the rise of what is called the 'surveillance society' (Marx 1985). In subsection 1.4.2 I shall describe the

8 Commissie Grondrechten in het Digitale Tijdperk 2000 (Commissie Franken).

theory of Panopticism, which is closely related to the idea of the surveillance society.

1.4.1 Six characteristic features of the Information society

Franken describes *dematerialisation* as a shift from physical goods and services to digital ones. Though Franken describes dematerialisation mainly as an economic issue restricted to goods and services, I would like to expand the concept of dematerialisation to the social realm. Human interaction is also 'dematerialising', since an increasing amount of human interaction is conducted over a geographical distance by means of telecommunication.

Globalisation thus ties in closely with dematerialisation. Social activity is no longer confined to the borders of the nation state and the jurisdiction of a single government, but extends far beyond that.

The Information society is a *turbulent* environment that is subject to quick, unpredictable changes. These changes can be attributed partly to technology, but can also be of a social, political, or economic nature. The high speed at which society keeps changing poses various problems to which governments seek remedy. Yet, law and regulation, one of government's strongest tools for co-ordination and control, is finding it hard to keep up with the rapid pace of developments, especially those of a technological nature.

Horizontalisation is a feature that characterises the shifting balance of power within the Information society. The information monopoly of governments, from which they derive part of their power to co-ordinate and control, is dwindling. Corporations, through ICT, now have access to information sources that were previously only available to governments. This reduces the power of governments and even shifts the power partly from the public to the private sector.

A fifth feature of the Information society is its *vulnerability*. Two examples of this vulnerability are (1) hacking incidents and (2) the millennium bug. Our world is increasingly dependent on the ICT infrastructure that underlies our Information society. The ICT infrastructure has become vital to our society and is indissolubly linked with important sectors of our society such as finance, logistics, energy, and healthcare. All these connections lead to interdependencies between different vital infrastructures and sectors.

A sixth feature of the information society is the notion of *transparency*. It describes the fact that data is being collected on individuals to such an extent, that a fairly clear profile of the corresponding persons can be made, thus rendering them transparent. Transparency is a result of the increasing application of surveillance in our (post)modern society. Surveillance can be described as the collection and processing of personal data, whether identifiable or not,

for the purpose of influencing or managing those, whose data have been garnered (Lyon 2001, p. 2). We rely on surveillance for the speed, efficiency, and convenience of many of our daily transactions and interactions. This is a direct result of the complex way in which we structure our political and economic relationships in a society that values security, consumer freedom, speed, mobility, and convenience (Lyon 2001, p. 2). Although surveillance is for the better part benevolent and conducted with the implicit or explicit consent of the subject it also has a 'darker side'. When third parties acquire data on individuals through surveillance, they gain a certain amount of power over them. While this power can be used for co-ordination, it can also be used to control a person or situation.

1.4.2 Panopticon

In 1791, social reformer and philosopher Bentham (1843), introduced a new type of penitentiary design that he called the Panopticon. The aim of this revolutionary prison design was to keep the inmates under close and continuous scrutiny. The prisoners were not allowed any private space and were watched at all times. Hence, Bentham named his prison design the 'Panopticon', Greek for 'all-seeing place'. The key to the Panopticon was the fact that the prisoners did not know if, or when, they were being watched. Through an intricate design of windows and shutters, the guards were shielded from view of the prisoners, who would thus come under the impression that they were continuously watched. Consequently, under these circumstances doubt and uncertainty would encourage obedience among the inmates, leading to a change in their behaviour. The Panopticon design was never (fully) adopted, although its principles were to have a significant impact on penitentiary practice.

Foucault (1975) revived the interest in the Panopticon with his seminal work *Discipline and Punish*. He described the shift in disciplinary control from brutal displays of power, such as public executions, to a more "subtle, calculated technology of subjection" (Foucault 1975, p. 201). For him the Panopticon was a means to "induce in the inmate a state of conscious and permanent visibility that ensures the automatic functioning of power" (Foucault 1975, p. 201). The actual exercise of power is no longer necessary, since the subjects are "caught up in a power situation of which they themselves are the bearers" (Foucault 1975, p. 201). The essence of surveillance according to Foucault is the accumulation of information and the direct supervision of subordinates (Lyon 1994, p. 66). The panoptic concept is therefore increasingly associated with current electronic surveillance practices, even though Foucault himself did not make this connection in *Discipline and Punish*. The electronic Panopticon, made possible by information and communication technology,

has the potential to restrict our freedom and autonomy, shifting the balance of power in favour of those who employ the surveillance techniques.

1.5 Privacy and liberty

If knowledge is indeed power, the amount of personal information available to third parties will for a large part determine to what extent power can be exercised over an individual. The rise of information and communication technology brought with it a fear that the accumulation of personal data by public and private parties would shift the balance of power away from the individual. The issue at stake thus seems to be the restriction of power and the preservation of our liberty. The defining idea of liberty is the absence of external restraints or coercion (Parent 1983, p. 274). Surveillance opens up new possibilities for restraint, coercion, and control, thereby creating a possible threat to liberty.

The opposite of surveillance in legal discourse is privacy. In law, privacy refers to a situation in which the private sphere of the individual is respected. Therefore, the private sphere should remain free from surveillance and interference by outsiders (Blok 2002, p. 323). Foucault's interpretation of the Panopticon illustrates the fact that the destruction of privacy plays an important role in the loss of freedom, autonomy, and individuality. The idea of the Panopticon is that a complete absence of privacy will stimulate socially acceptable behaviour. If individuals can retain (part of) their privacy, it will be harder for third parties to influence them.

Traditionally, the private sphere was made up of the home, the family life, and correspondence (Blok 2002, p. 323). Within these domains individuals are free to live their lives as they see fit. Since the right to privacy enables us to shield certain parts of our being from third parties, it also seems an ideal candidate for curbing the uncontrolled spread of personal data. Over the last few decades the private sphere has therefore grown to include personal data. By incorporating personal data into the private sphere, a new type of privacy emerged: informational privacy. Westin (1967, p. 7) defined informational privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated."

Privacy and liberty, though closely related, are two distinct values. In law, different mechanisms have evolved to protect both values, as I will show in the chapter on privacy and liberty. Whether (informational) privacy can provide the necessary protection against control, or if it can be applied to the use of software agents, is open to debate. Although the notion of informational privacy seems to be generally accepted as is the prevailing thought behind new laws governing the use of personal data, some scholars remain sceptical

about the value of privacy in the Information society.[9] I shall take their criticism into account when examining informational privacy and software agents.

Agents used for surveillance purposes form a potential threat to our privacy and ultimately our freedom. This threat will be stronger when the autonomy and authority of software agents increase. It is my belief that this threat can be effectively countered by regulating the use of software agents through norms and laws, effectuated, in part, in agent architecture. We may distinguish two situations in which software agents threaten the so-called 'informational privacy'. These are information retrieval *from* software agents and information retrieval *by* software agents.

1.5.1 Information retrieval from software agents

The first way in which agents can threaten privacy is when they surrender information willingly or unwillingly to third parties. In order to fulfil a given task, an agent must have certain information regarding the task at hand. If, for instance, I ask my software agent to send my mother a nice gift, it needs to know many things about my mother and me: my name, my mother's name, my mother's taste in gifts, her address *et cetera*. The agent needs this information to complete the transaction, so it will probably give this information voluntarily to the party with whom it is doing business.

An agent can also be tricked or forced into surrendering personal data regarding its user. If an agent is led to believe it is interacting with a trustworthy counterpart it can be tricked into revealing information. Apart from deceit, an agent can also become the victim of a deliberate attack. Like any software program an agent can be hacked, either by a human or a software agent that is stronger. When an agent is hacked, its contents will be revealed to the attacker (Borking 1998, p. 28-31).

A general assumption in agent research is that the more complex a task becomes, the more information an agent needs to carry it out appropriately. So the more powerful an agent becomes, the more (personal) data it will contain. Obviously, when an agent has a higher degree of autonomy and more authority is vested in it, the degree of direct control we have over it is less. This poses a potential risk to privacy. Moreover, the use of software agents which can generate data themselves, can lead to the creation and distribution of private information without knowledge of the user, thus denying the user control over his private information.

9 See for instance Lyon (1994), Blok (2002) and Stalder (2003).

1.5.2 Information retrieval by software agents

The second way in which agents may threaten the privacy is when third parties employ them against individuals. Third parties can obtain information on individuals by monitoring them, or by searching for recorded data on them (Lessig 1999, p. 143). Of all the tools that can be used for these tasks, agents are among the ones that look most promising. Agents obtain personal data on individuals from a variety of distributed data sources. They can obtain these data through obtrusive interaction, unobtrusive observation or unobtrusive searching. By obtrusive interaction I mean that in order to acquire data on an individual, the agent needs to interact actively with the user. In other words, the agent needs to ask the user for the information. In many cases this is undesirable, since it places a burden on the user, who might not like being disturbed in his work, or is unwilling to surrender any information to a third party agent. In the case of unobtrusive observation an agent does not engage in interaction with the user, but rather observes the user, recording any relevant information that is gathered during the observation for future reference, or to augment itself. An agent is conducting an unobtrusive search when it is searching and gathering information regarding the user from various sources, such as databases, cameras or other agents, without the user's knowledge or prior consent.

1.6 Problem definition

Given these prior considerations about privacy, liberty, agents, and control, we can use either one of the identified threats to define the problem to be discussed in the context of this thesis. I have chosen to focus my research on the threat posed by third parties employing agents to obtain information on individuals or groups. In order to establish a balanced problem definition I shall elaborate a bit further on the subject of information retrieval.

Storing data in electronic form is cheaper than in physical form. Besides this cost factor, the accumulated data is also more valuable because it can be accessed and processed more easily than data stored in physical form. These advantages, combined with the rapid drop in cost of digital storage space in the last decade, have driven both public and private parties to maintain extensive databases on almost every conceivable subject. Personal data (data related to an individual) is also stored in numerous databases. Apart from databases, the World Wide Web, newsgroups, IRC channels, and traffic data also contain a wealth of personal data. The sheer amount of data available in these heterogeneous, distributed data sources makes effective searching for information by means of direct manipulation virtually impossible. The volume of data thus becomes too great to yield information and knowledge, a problem known as 'information overload'.

The accumulation and interpretation of information by means of electronic surveillance is being hampered by information overload, therefore automated means of information gathering and knowledge discovery are used. Tools for selective pro-active as well as reactive information retrieval and knowledge discovery constitute some of the key enabling technologies for managing information overload (Yang 1998).

The use of data-analysis tools to discover patterns and relationships in data that may be used to make valid predictions is commonly referred to as 'data mining'. Interconnectivity and interoperability between systems, networks, databases, and other ICT applications, make it possible to obtain data from a host of different, distributed, heterogeneous data sources. Combining data from various types of distributed data sources can lead to valuable knowledge discovery or enrichment.

1.6.1 Three causes

Mining data, in general, is focused on finding patterns in large, pre-existing collections of data, not on finding information on individual subjects (Stanley 2003, p. 3). However, the collection of data using automated means also opens up possibilities for data mining on individuals. Mining data on a specified individual is known as *data surveillance* or *dataveillance*. It is the collection of information about an identifiable individual, often from multiple sources, that can be assembled into a portrait of that person's activities and preferences (Stanley 2003, p. 3). Until recently the possibilities for data surveillance were limited. We can identify three interrelated causes for this limited use of data surveillance by the government.

The first cause is a lack of adequate tools for effective and efficient data surveillance. Data surveillance requires special tools, such as agents, for automated data gathering and further processing. Besides special tools, system interoperability and interconnectivity are prerequisites too. Up till now, these tools were not available and the interconnection and interoperability of systems were quite limited. However, advances in computer science are quickly removing these barriers, bringing data surveillance ever closer to reality.

The second cause is a lack of inter-organisational cooperation. This means that while relevant data may be available in various intelligence and law enforcement agencies, it is not readily shared. A lack of inter-organisational cooperation was one of the main reasons why the September 11 attacks were not prevented. While sufficient information was available that suggested an imminent attack, the lack of co-operation and data-sharing prevented analysts from detecting the attack.

The third cause has a legal nature. The right to privacy is a human right, explicitly protected in a number of international treaties, and in the constitutions of almost every civilised nation in the world. The law places restrictions

on the automated processing of personal data. Needless to say, data surveillance is a potential threat to the privacy. In many countries the interconnection of databases is prohibited, because monitoring and profiling an individual then becomes a possibility.

1.6.2 How to safeguard privacy and liberty?

The lack of adequate tools and inter-organisational cooperation were *de facto* safeguards for the privacy and liberty of individuals. However, the proliferation of better tools for data surveillance and the improved cooperation within the intelligence community are events that are mutually strengthening. Together they will quickly remove any obstacles that previously acted as safeguards for privacy and liberty.

Eventually, it will be technically possible for software agents to profile and monitor people on an individual basis, both pro-active and reactive, opening up the possibility for extensive social orchestration and control. Without proper safeguards, parties will be able to acquire extensive knowledge on individuals and groups, which could have far reaching consequences for the balance of power in society.

When technological and organisational barriers are eventually removed, only the law remains to defend privacy and (individual) liberty. However, the current legal framework assumed to be still active, could be inadequate, due to the fact that it was put in place before the software-agent paradigm emerged. Owing to their unique characteristics (autonomy, adaptability, *et cetera*), software agents form a break with existing means of knowledge retrieval, posing not just a quantitative difference, but also a qualitative difference with existing means of electronic surveillance.

1.6.3 The precise formulation

Taking into account the above reasoning we arrive at the following problem definition:

Is it possible to maintain privacy and liberty in a society where software agents are able to overcome the information overload?

1.7 Research goals and research questions

Using the problem definition as both starting point and guideline, I shall set out to accomplish the following research goals.

1 Adequate evaluation of the legal framework for the protection of privacy and liberty in the light of software agent technology.
2 Adequate amendments, where necessary, to the legal framework for the protection of privacy and liberty, by taking into account the use of software agents for surveillance purposes.

In order to reach these research goals I shall try and answer the following four research questions during the course of this thesis.

1 *How will agent technology influence the surveillance practice?*
2 *How will the use of agent technology impact privacy and liberty?*
3 *How will the use of agent technology impact the legal framework for the protection of privacy and liberty?*

and

4 *In order to safeguard privacy and liberty, how must the use of software agents be regulated?*

1.8 Research approach

Since the subject matter of this thesis deals with issues that have their basis amongst others in computer science, sociology, psychology, and law, I feel that it is necessary to adopt a multi-disciplinary approach when it comes to answering the research questions and attaining the research goals.

The first part of the thesis (chapters 2 through 6) will be used to provide background information from various fields of science on the three basic elements that make up this thesis: (1) software agents, (2) surveillance, and (3) privacy. The development of technology, in particular artificial intelligence technology, plays an important role in the future development of surveillance. Therefore, chapter 2 and chapter 4 have been written from a computer science perspective. Chapter 3, which deals with surveillance and the impact of technology on society and the individual, has been written from a sociology and psychology perspective. Chapters 5 and 6 have been written from a legal perspective, but also contain ideas from political science and philosophy.

In the second part of this thesis (chapters 7 through 10) the ideas from computer science, sociology, psychology, and law will be merged into a coherent whole. In chapter 7, I shall take the insights from computer science gained in chapter 2 and 4, and those from sociology gained in chapter 3, to describe how they affect (the legal framework for) privacy and liberty as described in chapters 5 and 6. Chapters 8 and 9 will then approach the issues primarily from a legal perspective, since this thesis deals first and foremost with the legal framework for privacy and liberty.

1.9 THESIS OVERVIEW BY CHAPTER

In chapter 2, I shall explore the agent phenomenon. Only when we have a comprehensive understanding of agent technology and its applications, we can try and identify the threats posed by software agents to privacy and liberty. I shall give a description of the various types of agents, their applications, and the way they operate, by studying literature on agents, as well as looking at current real-world applications of agent technology. My research will focus on the use of agents to overcome the limitations of current user interface approaches in general, and agents used for monitoring and data processing in particular. I shall also discuss general legal issues on agents, in view of the fact that these issues are relevant when it comes to software agents and privacy.

In chapter 3, I shall examine the issue of surveillance and its relation to control. I shall describe the use of surveillance as a disciplinary tool as well as the use of surveillance in a more liberal setting where it is used for added security, convenience, or to enable better risk management. I shall also discuss the trend towards system integration and function creep that may lead to the rise of a 'maximum surveillance society'. I shall conclude the chapter by discussing the use of synoptic surveillance as a possible means to restore the balance of power between the watchers and the watched.

In chapter 4, I shall describe how software agents may be employed to facilitate surveillance practices. Real-world applications as well as possible future applications will be discussed in order to gain a greater insight into the phenomenon of agent use and its influence on privacy and liberty.

In chapter 5, I shall discuss the various conceptions of privacy and the dimensions to which they apply. I shall also discuss how the right to privacy has developed over time in response to technological changes. The chapter will be concluded with a description of privacy in substantive law. I shall describe the legal framework for surveillance and privacy of both the Netherlands and the United States. By examining the legal framework of both a civil law country and a common law country we can make a better assessment of how agent-enabled surveillance will impact the legal framework for privacy and liberty.

In chapter 6, I shall explore the relationship between privacy and liberty. Using the negative and positive concepts of liberty I shall argue that privacy is an important means of protecting liberty. However, I shall also argue that privacy should not be the only method of protecting liberty in the information society.

In chapter 7, I shall determine what the effects of agent-enabled surveillance are on privacy and liberty. In doing so, I shall distinguish between quantitative and qualitative effects of agent-enabled surveillance.

In chapter 8, the current legal framework will be reviewed in the light of agent technology. I shall describe the legal issues that result from the quantitative and qualitative effects of agent-enabled surveillance.

In chapter 9, I shall determine how the legal framework for the protection of privacy and (individual) liberty can be changed or amended in order to deal with the effects of agent-enabled surveillance. Moreover, I shall discuss how possible changes to the legal framework can be effectuated best.

Chapter 10 will conclude this thesis and provide suggestions for future research.

2 Software agents

The future is already here,
It's just not very evenly distributed.
William Gibson

The purpose of this chapter is to describe agent technology and its possible applications. With a greater understanding of agent technology, we can determine whether the software agent paradigm will fundamentally alter the way in which surveillance can be conducted.

First I shall give a general overview of artificial intelligence in section 2.1. Next I shall illustrate the need to situate artificial intelligence in an environment in section 2.2. The notion of agency, central to modern artificial-intelligence research, will be the subject of section 2.3. The various characteristics commonly attributed to software agents will be the topic of section 2.4. I shall describe various agent typologies in section 2.5, software agent architecture in section 2.6, and multi-agent systems in section 2.7. After the description of the technical side of software agents, I shall turn to the future of software agents. In section 2.8 I shall describe the projected timeline for the continuing development of agent technology. In section 2.9 I shall place the agent phenomenon in the broader perspective of 'ambient intelligence'. I shall end the chapter with a discussion on some of the legal issues that have arisen as a result of the agent-technology paradigm in section 2.10. Provisional conclusions will be drawn in section 2.11.

2.1 Artificial intelligence

Before we turn to the subject of software agents it is necessary to gain more insight into the field of artificial intelligence as software agents make up part of this field of research. Artificial intelligence is defined by Kurzweil (1990) as:

> "The art of creating machines that perform functions that require intelligence when performed by people."

Artificial-intelligence research thus aims at recreating within machines the mental processes normally seen in humans. A generally accepted definition of natural, human intelligence is given by Wechsler (1958):

> "The aggregate or global capacity of the individual to act purposefully, to think rationally, and to deal effectively with his environment."

We may regard Turing's (1950) article *Computing Machinery and Intelligence* and Shannon's (1950) discussion of how a machine might be programmed to play chess as the birth of artificial-intelligence research (van den Herik 1983, p. 95). Turing (1950, p. 433) was the first researcher to pose the question whether machines (i.e., computers) could think. Turing felt this question would be almost impossible to answer due to problems with the definition of the word 'thinking'. Turing avoided the philosophical debate on how to define 'thinking' by substituting the original question by a test (the imitation game) that can be used to determine subjectively whether a machine is intelligent. In the imitation game (now known as the Turing test), an interrogator has typewritten conversations with two actors he cannot see, one human, the other a machine. If after a set period of time the interrogator is unable to distinguish between man and machine on the basis of the conversation, the machine can be considered to be intelligent.

Since Turing's (1950) seminal work, impressive feats of intelligence have been accomplished in areas such as theorem proving, game playing, and decision making (Kemal 2006). However, half a century of artificial-intelligence research has failed to deliver the 'strong' artificial intelligence envisaged by Turing. The inability to approach humanlike intelligence lies primarily in the limitations of the 'classic' approach to artificial intelligence.

'Classic' or 'symbolic' artificial intelligence is the branch of artificial-intelligence research that attempts to represent knowledge in a declarative form (i.e., symbols and rules). It is based on the premise that the foundation of human cognition lies in the manipulation of symbols by the brain and that this process can be mimicked by a computer (Postma 2003, p. 6). A symbol is a mental representation of a real-world object (for instance, a table, a dog, or a flower) that is made up of patterns of active and inactive neurons. In a computer these patterns of active and inactive neurons can be substituted by sequences of zeroes and ones.

By representing knowledge in the form of symbols and using rules to guide the manipulation of these symbols, machines can be endowed with intelligence. In order for a computer to display intelligent behaviour it needs to have an internal symbolic representation of the world as basis for its actions (Luck 2004, p. 14). Symbolic artificial intelligence can be seen as a top-down approach to artificial intelligence in view of the fact that the entire state of the world needs to be completely and explicitly represented (Brooks 1991a, p. 140).

While the symbolic artificial-intelligence approach has yielded impressive results in specialised areas where the environment can be accurately modelled, it falls short when the size and complexity of an environment increases. The reason is that it is difficult, if not impossible, to represent a dynamic and complex environment -or even an abstraction thereof- comprehensively. This also goes for the representation of some symbolic manipulation tasks such as planning (Luck 2004, p. 14). Therefore the symbolic artificial-intelligence approach does generally not fare well within complex, real-world environments. However, the ability to deal effectively with the environment is a prerequisite for strong artificial intelligence.

2.2 SITUATED INTELLIGENCE

According to Wooldridge (2002) the history of computing has been marked by five important and continuing trends: *ubiquity*, *interconnection*, *intelligence*, *delegation*, and *human-orientation*. The first trend is a result of the reduction in the cost of computing. The low cost of computing power allows for its incorporation into a host of different (everyday) devices making computing progressively more ubiquitous. The second trend is towards the interconnection of computer systems into large networked and distributed systems such as the internet. The third trend is towards the creation of progressively intelligent computer systems able to perform increasingly difficult and complex tasks. The fourth trend is towards the delegation of control from the human actor to the computer. The fifth trend is towards the creation of computer interfaces that more closely reflect the ways in which humans act with their surroundings. Together these five trends make for an increasingly complex computing environment in need of intelligent systems that can deal effectively with it.

As described in the previous section, the limitations of symbolic artificial intelligence oftentimes prevent it from being used in real-world environments. A new approach to artificial intelligence was needed to overcome the fundamental problems that faced symbolic artificial intelligence. The new approach to artificial intelligence draws inspiration from cybernetics and biology. It is based around two ideas, *viz.*

- that intelligent, rational behaviour is seen as innately linked to the environment an agent occupies;
- that intelligent behaviour emerges from the interaction of various simpler behaviours (Wooldridge 2002, p. 89).

The first idea, of situated intelligence, forms a break with the traditional symbolic artificial-intelligence approach. It is based on the premise that intelligent behaviour is not disembodied, but that it is a product of the interaction an artificial-intelligence system maintains with its environment (Wooldridge

2002, p. 89). This premise seems to be consistent with the idea that one of the constituents of intelligence is the ability to deal effectively with the environment. Instead of having an internal representation of their environment, situated artificial-intelligence systems (i.e., agents) use sensors to observe their surroundings and actuators to interact with it. Using sensors to observe the world largely eliminates the need for symbolic representation because "the world itself is its own best model" (Brooks 1991b, p. 4). The world that an agent inhabits can be either the physical world or a software environment like the internet. Agents operating in the physical world (such as robots) are called situated agents, while agents operating in a software environment are called software agents (Postma 2003, p. 14).

The second idea is largely inspired by Minsky's (1986) work. Minsky's argument, which he puts forth in his book *The Society of Mind*, is that the human mind is made up of many small, unintelligent processes. Minsky calls these processes agents, though they should not be confused with the software agents discussed in the context of this thesis. It is through the interaction of different agents that intelligent behaviour emerges (Minsky 1986, p. 17). Inspired by Minsky's ideas, Brooks (1991b) argued that higher-level intelligence need not be programmed directly into a machine from the top down, but can emerge from the interaction of multiple simple modules situated within a real environment. Brooks formalised Minsky's ideas into an agent architecture known as the subsumption architecture (1991b). It works by placing a combination of hierarchically organised, augmented finite state machines (i.e., agents) in an environment where they can interact with each other and their surroundings.[1] Through the interaction of the individual finite state machines complex behaviour may emerge.

As we can judge from these two important ideas, agents are central to the new approach in artificial intelligence. Therefore, it is important to continue exploring the notion of agency.

2.3 Agency and autonomy

In general, an agent can be seen as an entity that causes an effect or exerts some form of power over its surroundings. Since such a broad definition of agency applies to almost everything in our physical surroundings ranging from chemical substances to human actors, it is necessary to formulate a more narrow definition of agency for the context of this thesis. Such a definition of agency could be that of an entity that acts or has the power or authority to act or represent another. In this sense the notion of agency is primarily concerned with delegation. While in general applied to human relationships,

1 The finite state machines are augmented with timers and a mechanism for distributed control so they are able to display coherent, continuous behaviour.

this notion of agency can also apply to computer programs. By a software agent we thus mean a computer program that behaves in a manner analogous to a human agent (Etzioni and Weld 1995, p. 45). Instead of the human actor it is the software program that carries out the task, because the task is perceived to be either too tedious or too difficult to be performed by a human actor.

According to Gilbert (1995) agency is the degree of autonomy and authority vested in a software agent. In others words, in order to meet their design objectives agents must be able to operate without the direct intervention of humans and should be in control of their own actions and internal state (Jennings and Wooldridge, 1998, p. 4). However, the mere fact that an entity is able to function autonomously is by itself not sufficient for that entity to qualify as an agent. Jennings and Wooldridge (1998, p. 4) describe software agents as computer systems capable of *flexible* autonomous action in order to meet their design objectives. This flexibility determines the difference between agents and mere objects. Agents have thus been proposed as situated and embodied problem solvers that are capable of flexible and autonomous action (Luck 2004, p. 3).

It is the capability for flexible and autonomous action that distinguishes agents from objects. An object has some control over its state (i.e., it can only be accessed or modified via the methods that the objects provides), but not over its own behaviour. When properly addressed (by another object or an agent) the object will simply execute the requested task, it has no control over the execution of its methods. When I flip a light switch, I use the proper methods defined by the light switch and can therefore access it. From here on, the light switch has no further say in the execution of its methods and must respond by turning on the light. An agent, however, actually has a say (based upon the knowledge and parameters defined in its internal state) in the execution of its own methods (Luck 2003, p. 10). Only when a request made by another agent or object is in accordance with its design objectives, the agent will execute the request. The requesting agent or object also has no control over the execution of the agent's methods. This authority resides within the agent itself therefore we tend to believe we *request* an action from an agent, while we *access* objects (Jennings and Wooldridge 1998, p. 4).

Flexible autonomous agents are already being used for a variety of different tasks ranging from the autonomous control of spacecrafts (Das *et al.* 2002) to personal digital assistants (FIPA 2001). The area of application that is of special interest to the subject matter of this thesis is the use of software agents for surveillance practices. In this field agents are primarily used for data processing and automated monitoring. I shall examine the use of agents for surveillance purposes more in depth in chapter 4.

2.4 AGENT CHARACTERISTICS

The difficulty in accurately defining software agents lies primarily in the fact that people tend to have different associations with the notion of agency. As Russel and Norvig (1995, p. 33) point out: "the notion of an agent is meant to be a tool for analysing systems, not an absolute characterisation that divides the world into agents and non-agents". Therefore, 'software agent' or 'intelligent agent' can best be seen as an umbrella term for programs that to some extent display attributes commonly associated with agency (Nwana 1996, p. 2). In this section I will elaborate further on these characteristics.

Although opinions differ as to what is an accurate description of a software agent, we can discern some common characteristics that appear in various software agent definitions. By enumerating these characteristics we can increase our understanding of the defining elements of agency. Below we discuss seven characteristics, *viz.* (1) reactive, (2) pro-active and goal-oriented, (3) deliberative, (4) continual, (5) adaptive, (6) communicative, and (7) mobile. An agent need not display all seven characteristics to be considered an agent. It is rather that when a software entity has a number of the characteristics mentioned in this section, it will be generally regarded as a software agent.

2.4.1 Reactive

In order for an agent to function autonomously in any given environment it must be able to perceive its environment and act in a timely fashion upon changes that occur in it (Wooldridge and Jennings 1995, p. 4). A software agent may employ any type and number of sensors to sense its environment. The agent can react to sensory input using its actuators. We can differentiate between various degrees of reactivity, ranging from purely reactive software agents on the one hand, to software agents that deliberate extensively before reacting on the other hand. I shall elaborate further on this characteristic in section 2.6 when I discuss agent architectures.

2.4.2 Pro-active and goal-oriented

Pro-activity is a more specialised form of autonomy. When an agent is said to be pro-active, it does not simply act in response to its environment, but it will exhibit goal-directed behaviour and take initiative to attain its goals or design objectives (Wooldridge and Jennings 1995, p. 4). According to Maes (1995b, p. 108) a definition of software agents could be:

> "computational systems that inhabit some complex dynamic environment, sense and act autonomously in this environment, and by doing so realize a set of goals or tasks for which they are designed."

This definition of software agency combines the characteristics autonomy and reactivity and introduces goal-oriented behaviour as a further requirement. Goal-oriented behaviour is the ability on the part of a software agent to work towards attaining goals specified in advance. This behaviour goes beyond mere reactivity and demands a pro-active demeanour from the agent.

2.4.3 Deliberative

More sophisticated agents are not merely reactive (i.e., operating in a stimulus-response manner) but are able to reason about their actions. The ability to reason enables agents to act pro-actively and perform more difficult tasks in complex environments. I shall examine deliberative agents more closely in section 2.6.

2.4.4 Continual

In order for a software agent to accomplish its goals, it must have temporal continuity. The agent must be able to function over a certain period of time with persistence of identity and state. Agents that have an episodic memory are able to learn from previous experiences (Bradshaw 1998, p. 8).

2.4.5 Adaptive

When discussing autonomy we saw that Jennings and Wooldridge (1998) distinguished between objects and agents in terms of flexibility. Making agents adaptive is one way of attaining flexibility. Adaptivity can range from (1) being able to adapt flexibly to short-term, smaller changes in the environment, to (2) dealing with more significant and long-term (lasting) changes in the environment (Maes 1995a, p. 3). Software agents that are able to deal with long-term changes are able to improve themselves and their performance over time by storing the knowledge of past experiences within their internal state and taking this knowledge into account when executing (similar) actions in the future.

2.4.6 Communicative

Agents should be able to communicate with other software agents and even humans in order to complete their tasks and help other agents complete theirs (Jennings and Wooldridge 1998, p. 5). Especially in multi-agent systems the ability to communicate with other agents is important. Agents communicate with other agents using a common agent language, such as FIPA ACL or KQML. When agents communicate with humans they must communicate using natural language.

2.4.7 Mobile

A final characteristic often associated with software agents is mobility. Although mobility is neither a necessary nor a sufficient condition for agency, many scholars (Gilbert *et al.* 1995; Nwana 1996; Brazier *et al.* 2003) include mobility when describing agent characteristics.

It is oftentimes better for an agent to interact with a remote system at the location of the remote system than to do it over a distance. Several reasons for this preferred form of interaction can be specified. A first reason is efficiency. Network traffic can be reduced when the agent and the remote system are at the same location. For instance, when an agent queries a remote database, data has to be sent back and forth between the remote database and the agent. This communication can be kept local when the agent and the remote system are at the same location, thereby reducing the strain on external networks such as the Internet. A second reason is that data need not be exchanged over (public) networks but can be handled locally. It also means that agents can operate more secure. A third reason is that the remote system only allows for agents to operate locally, thereby forcing the agent to migrate to the remote location.

2.5 AGENT TYPOLOGIES

Software agents may incorporate any number of the characteristics mentioned in section 2.4 into their design depending on the demands of the environment and the task at hand. This leads to a continuous spectrum of different agent types. Several attempts have been made (Wooldridge and Jennings 1995; Gilbert *et al.* 1995; Franklin and Graesser 1996; Nwana 1996; Luck 2003) at providing more insight into this continuous spectrum by establishing agent typologies that classify different types of agents according to their characteristics and architecture.

Wooldridge and Jennings (1995, p. 4) divide agents into those with a weak notion of agency and those with a strong notion of agency. The strong notion

of agency is primarily associated with a higher level of intelligence. The stronger notion of agency is represented in the ability to reason using mentalistic notions such as knowledge, belief, desire, intention, and obligation.

Gilbert (1995) classifies software agents using three dimensions: agency, intelligence, and mobility. Agency, as mentioned before, is the degree of autonomy displayed by the agent and the amount of authority vested in it. Intelligence is the degree of reasoning and learned behaviour: the agent's ability to accept the user's statement of goals and carry out tasks delegated to it (Bradshaw 1998, p. 9). Higher levels of intelligence refer to characteristics such as adaptivity and deliberation. Mobility is the agent's ability to move from one location or agent platform to another. It is along these three dimensions that Gilbert maps out different types of agents.

Using a fairly broad definition of agency as a starting point, Franklin and Graesser (1996) set out to distinguish between different types of agents on the basis of (1) their control structures, (2) the environment in which they operate, (3) the language in which they are written, and (4) their applications.

Nwana (1996) uses multiple dimensions to define different types of agents. These dimensions include mobility (static versus mobile), the presence of a symbolic reasoning model (reactive versus deliberative), the display of primary attributes (such as autonomy, cooperation, and learning), the display of secondary attributes (continuity, trust, emotional qualities), different roles, and hybrid agent types (that combine multiple characteristics).

Luck (2003, p. 12) makes a broad distinction between different types of agents based primarily upon agent architecture. Luck places purely reactive agents on one end of the spectrum and deliberative agents on the other end. In between we find the hybrid agent class that combines both reactive and deliberative elements into their architecture.

As is to be expected, none of these typologies can fully incorporate and classify all software agent types and applications. Rather, the different typologies aid in distinguishing between different types of agents and their possible applications. For the context of this thesis the most important thing we can learn from the various typologies is that there is a difference in the levels of intelligence that agents can display. This is important because agents with higher levels of intelligence (i.e., displaying characteristics such as deliberation, adaptivity, and pro-activity) are more likely to alter the way in which information is gathered and processed, which in turn might pose a more serious threat to privacy and liberty. The level of intelligence is determined by the agents architecture therefore we shall now turn our attention to agent architecture.

2.6 AGENT ARCHITECTURES

Agents are able to display the characteristics mentioned in section 2.4 through their program architecture. A host of different agent architectures ranging from

the mundane to the highly complex endow software agents with the ability to 'act' and 'think'. In general we can differentiate between three basic architectures: the reactive agent architecture, the deliberative agent architecture, and the hybrid or layered agent architecture (Luck 2004).

The distinction in architecture is based upon the way software agents react to their environment. Software agents perceive the environment in which they operate either through sensory input or by using an internal model of their surroundings. The software agent uses the information regarding its surroundings as the basis for its decisions. An agent can reach a decision through a reactive process, a deliberative process, or a combination of both. The agent executes its decision using its actuators.

2.6.1 Reactive agents

Reactive agents are a class of agents that do not possess internal, symbolic models of their environments and do not use complex symbolic reasoning to accomplish their goals; instead they act in a stimulus-response manner to the present state of the environment in which they are embedded (Nwana 1996, p. 25). Reactive agents do not plan their actions, but react directly to sensory input using a simple rule based if-then system. When an input signal exceeds a certain threshold, the agent is triggered into a predefined action.

A reactive agent can respond to changes in its environment in near real-time, making it very useful in environments that require quick responses from an agent. A drawback of the reactive agent architecture is the inability of reactive agents to do long-term planning. Since reactive agents act on impulse, either strongly or weakly displaying goal-oriented behaviour is difficult for them. Therefore, reactive agents are generally not considered to be intelligent and ill-suited for complex tasks.

2.6.2 Deliberative agents

Deliberative agents are a more sophisticated class of agents. This type of agent is able to reason about its behaviour and adapt to changes in its environment using an internal reasoning model. In addition to such a model, a world model can also be employed. The agent can use this world model to increase its chances of coming up with a successful plan in unforeseen situations. In general, deliberative agents can be seen as more intelligent. A trade-off to this increased intelligence is the inability to function in (near) real-time. Deliberative agents need more time for tasks such as computing input, matching and updating the internal state, and choosing an appropriate response. In other words, deliberative agents need more time to think.

The most successful deliberative agent architecture model is the BDI model and many deliberative agents are based on this model of agency. The BDI model reflects three mental attitudes namely *belief*, *desire,* and *intention*. *Belief* is the informative component of an agent's internal state and reflects the agent's information about the environment that it inhabits (Rao and Georgeff 1995, p. 3). The *desires* of an agent reflect its goals, motivations, and priorities. Finally, an agent's *intentions* make up the deliberative component of the agent; it includes planning and decision making capabilities.

2.6.3 Hybrid agents

Between the reactive agents and the deliberative agents we find the hybrid (or layered) agent class (Luck 2003, p. 12). Since both reactive and deliberative agents have their individual strengths and weaknesses, architectures are being developed that adopt the strong points of both. The motivation for building hybrid-agent architectures lies in the fact that a hybrid-agent approach is useful when either the reactive or the deliberative agent architecture alone is not fit for the designated task. Hybrid agents combine elements of reactivity with those of deliberation through an architecture that is divided into layers that each perform different functions.

2.7 MULTI-AGENT SYSTEMS

Up until this section we have concerned ourselves mainly with solitary agents. However as we have seen in section 2.2 there is a growing need for situated agents that can interact with other actors, both human and artificial.

Multi-agent systems (MAS) are systems wherein multiple (software) agents can potentially interact. The corresponding subfield of artificial intelligence that deals with the principles and the design of multi-agent systems is called distributed artificial intelligence (Vlassis 2003). Multi-agent systems provide several advantages over 'single-agent systems' (Stone and Veloso 1997). Below I shall discuss five of these advantages.

Efficiency
Having a system with multiple agents allows for parallel and asynchronous computation. In a multi-agent system tasks can be broken down into several independent tasks and computed simultaneously by different agents (Vlassis 2003, p. 4).

Robustness
Multi-agent systems can have built-in redundancy. If the responsibility for certain tasks is shared among different agents, the system can tolerate failures

from individual agents. By contrast when a single-agent system, daemon, or program fails, the entire system fails. Although a multi-agent system need not be implemented on multiple processors, to provide full robustness against failure, its agents should be distributed across several machines.

Scalability
Multi-agent systems are more flexible and scalable than single-entity (monolithic) systems. As a result of the modular approach of multi-agent systems, new agents can easily be introduced in the system giving it added capabilities.

Simpler programming
The modularity of multi-agent systems makes programming easier and allows for better control of the programming tasks. Rather than handling the whole task with a centralised agent, programmers can identify subtasks and assign control of those subtasks to different agents.

Emergent behaviour
By letting multiple (reactive) agents interact within an agent system, 'smartness' can arise out of the emergent behaviour of the interactions of the various modules (Nwana 1996, p. 27). As we have seen in the sections 2.1 and 2.2 this 'bottom-up' approach to artificial intelligence is steadily gaining prominence and is considered to be a valuable alternative to the 'top-down' approach of fully programming an artificial-intelligence system using symbolic reasoning and symbolic representation.

2.7.1 Architecture and standardisation

In order for agents and agent systems to interact they must be interoperable. While many different multi-agent systems are currently being developed independently, the use of common agent standards will improve interoperability and stimulate overall system integration.

There are two main standardisation efforts with regard to software agents and multi-agent systems, namely FIPA and KQML. The latter is part of the larger DARPA-sponsored Knowledge Sharing Effort focused on developing techniques and tools to promote the sharing of knowledge in intelligent systems (Finin *et al.* 1992). KQML, short for Knowledge Query and Manipulation Language, was designed to enable the sharing and reuse of knowledge bases and knowledge-based systems but was rapidly adopted by agent researchers. The Foundation for Intelligent Physical Agents (FIPA) was formed in 1996 to produce software standards for heterogeneous and interacting agents and agent-based systems. FIPA currently has the broadest user base, so I shall use the FIPA standard set to discuss multi-agent system architecture further.

The FIPA standardisation effort is based around the *FIPA Abstract Architecture* that acts as an overall description of the FIPA standard set (Luck 2004, p. 135). The primary focus of the Abstract Architecture is to create a (semantically) meaningful message exchange between agents that may be using different messaging transports, different communications languages, or different content languages (FIPA 2002a, p. 4). The Abstract Architecture focuses on the core interoperability of agents by providing designers with abstract agent-architecture components on which to base their concrete multi-agent-system implementations.

The management of agents is the main topic of the *FIPA Agent Management Specification* (FIPA 2002b). The Agent Management Specification defines (1) the type of environment that an agent inhabits, (2) the services that are expected to be available to it, and (3) the management actions that can be carried out by or for them (Luck 2004, p. 136). One of the elements often used in concrete implementations of the Abstract Architecture is the agent platform as described in the Agent Management Specification. Agent platforms are commonly used to provide the following services (Brazier *et al.* 2003, p. 4):

- creating and running an agent;
- searching for an agent;
- migrating agents to other platforms;
- enabling communication with other agents hosted by an agent platform.

In order for agents to interact on a given agent platform they must be able to communicate with each other. Effective interaction is the exchange (communication) of information and knowledge that can be mutually understood. To this end agents must share a common language and have a common understanding of the terms used in a given context. A third requirement is the ability to exchange both the message and the meaning between each other (Bradshaw 1998, p. 292).

There are a number of FIPA standards that deal with agent communication. A common language is provided in the form of *FIPA ACL* (FIPA 2002c). Common understanding (i.e., semantics) is provided in the form of a library of communicative acts or performatives (FIPA 2002d) that define formal and informal meanings for a set of different communicative acts specified by FIPA (Luck 2004, p. 139). The ability to exchange messages is standardised by the *FIPA Agent Message Transport Service* (FIPA 2002e).

Apart from these core specifications, there are numerous other FIPA specifications (ninety six in total, some of which are obsolete) that govern multi-agent-system design.

2.8 From closed to open systems

Research into agent technology started in the early 1980s and has since then evolved into an important field of artificial-intelligence research. As a result software agents and multi-agent systems are being used in many areas of our society. For now these systems are mostly closed, meaning that they are only applied in specific environments and do not interact with other agent systems. The challenge for the coming years will be to move away from these closed systems towards more open and scalable multi-agent systems that allow agents to travel from one agent system to another and learn new skills on the way.

It is important to gain a clear vision on the future of agent technology if we are to assess the impact that software agents may have on surveillance. Such a vision on the future development of agent technology is set out in the *Agentlink Roadmap* (Luck *et al.* 2003, p. 33). I shall use the Agentlink Roadmap to describe briefly the move towards open and fully scalable systems that are inhabited by increasingly intelligent agents.[2] The Agentlink Roadmap distinguishes four phases.

2.8.1 Phase I: Closed agent systems (2005-2008)

The present deployment of software agents and multi-agent systems can be best characterised as *closed*. The current breed of agent systems is usually employed within a single (corporate) environment with participating agents sharing common high-level goals within this domain (Luck *et al.* 2003, p. 34).[3] Usually the software agents used in closed agent systems are not quite intelligent, this is not only due to the current limitations of agent technology but is also an issue of trust: people do not yet feel comfortable with the idea of intelligent, autonomous software applications (Schermer, Durinck and Bijmans, 2005).

2.8.2 Phase II: Cross-boundary systems (2008-2012)

In the second phase of the agent-technology development, systems will increasingly be designed to cross the borders of individual organisations, though typically it will still be a single design team that develops an agent system. While agents in this phase might have fewer goals in common they will still operate within a single domain and share common domain knowledge (Luck

2 However, my estimation of the timeline for the development of agent systems will be more conservative.

3 One exception to this general rule is the extensive use of simple agents on the internet.

et al. 2003, p. 34). Standardisation of communication and interaction protocols such as defined by the FIPA will become evermore important.

2.8.3 Phase III: Open systems (2012-2015)

In the third phase (medium-term future) we will see more systems that are open. These systems will allow multiple heterogeneous agents from different design teams to operate on the same agent platform, provided the agents adhere to the publicly stated requirements and standards of the agent platform (Luck *et al.* 2003, p. 35).

2.8.4 Phase IV: Fully scalable systems (2015 and beyond)

The final phase of software-agent development will see fully scalable systems capable of supporting almost limitless amounts of agents. It is likely that in this phase agents will be highly mobile, pro-active, and capable of learning new skills on the entry of a system. The agents will thus be more intelligent and capable of performing more difficult tasks. It is to be expected that over time people will have grown to be accustomed to the use of intelligent, autonomous agents and will no longer have fears when it comes to employing agent technology.

2.9 AGENT DEVELOPMENT IN BROADER PERSPECTIVE

It is likely that software agents will become an important element of our everyday life in the near future. As mentioned in section 2.2 the history of computing has been marked by five important and continuing trends: *ubiquity*, *interconnection*, *intelligence*, *delegation*, and *human-orientation*. These trends are made possible by a range of new technologies such as Radio Frequency Identification (RFID), embedded systems, grid computing, swarm intelligence, and nanotechnology. These technologies will allow for the integration of machine intelligence with our everyday environment. Eventually this development will constitute the next big ICT paradigm, that of ambient intelligence (AmI). Ambient intelligence, or ubiquitous computing, is a vision of the future of the information society where we will be surrounded by intelligent and intuitive interfaces embedded in everyday objects around us and an environment recognising and responding to the presence of individuals in an invisible way (Ahola 2001).

The role that software agents could play in the ambient-intelligence vision is twofold. First, software agents could be used to take up the difficult task of managing the complex networks and computing environments that will

evolve as a result of ambient intelligence. The second role software agents could play is in the interaction between the human actor and his intelligent environment. Interface agents could provide a pleasant and intuitive way to interact with complex and intelligent environments.

2.10 Legal issues on agents

As software agents typically operate in a real-world environment there is a significant chance that they perform actions to which the law applies. The legal implications of their actions are, however, not well understood (Brazier *et al.*, 2002). These legal implications touch upon a number of subjects that range from liability to intellectual property. In this thesis I shall confine myself to a discussion on those legal issues that are most relevant to the subject matter of this thesis. In my opinion there are four issues to be discussed, *viz.* (1) autonomy, (2) legal status of agents, (3) identification, authentication and authorisation, and (4) integrity.[4]

2.10.1 Autonomy

When it comes to discussing legal issues surrounding the use of software agents, the first issue that needs to be addressed is that of software agent autonomy. Above all, it is important to distinguish between what I will call the *technical* notion of autonomy and the *legal* notion of autonomy. From a computer science perspective the term autonomy is primarily concerned with a software agent's ability to function without external help or guidance. However, from a legal point of view the notion of autonomy is less concerned with the *ability* to act, but rather with the *authority* to act (Schermer, Durinck and Bijmans, 2005, p. 14). The notions of technical and legal autonomy are closely entwined. A software agent capable of advanced autonomous actions must also have the authority to do so, and a software agent that has a broad mandate, must also have the technical means to fill in this mandate.

2.10.2 Legal status of agents

Closely related to the issue of autonomy is that of the legal status of software agents. With regard to the role of software agents in commercial transactions and criminal law it is still unclear whether an agent must be seen as a natural

4 These legal issues are closely related to Franken's *'Beginselen van behoorlijk ICT gebruik'* (principles of proper ICT use) (Franken *et al.* 2004, p. 57). The principles are: availability, confidentiality, integrity, authenticity, flexibility, and transparency.

person (which is unlikely), a legal person, or whether it has any legal subjectivity at all.

In Dutch law the notion of a software agent as a separate legal entity has not yet arisen. In the United States however, there is a clear reference to the notion of software agency in the *Uniform Electronic Transaction Act* (UETA), developed by the National Conference of Commissioners on Uniform State Laws (NCCUSL). Section 2 (6) of the UETA defines an 'electronic agent' as:

> "a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual."

When it comes to the legal status of a software agent, the notion of agency is important. Agency in a legal sense is the relationship between the principal and the agent, based on authority, or the power conferred on the agent to constitute legal relations between the principal and a third party (De Miglio *et al.*, 2002).

2.10.3 Identification, authentication, and authorisation

The ability to identify and trace a software agent is important both from a technical and a legal point of view. From a technical standpoint the ability to identify an agent is necessary to coordinate the workings of a multi-agent system. Technical identifiers are used among other things for the discovery of agents and to coordinate communication between agents.

From a legal standpoint it is often beneficial, if not necessary or even compulsory, to be able to identify oneself. It is conceivable that software agents should carry some kind of marker (akin to a licence plate) that enables their identification and that of their principal in certain circumstances (Brazier *et al.* 2003, p. 37). Since an agent is capable of autonomous action, it might perform acts in law. An agent could, for instance, cause damage when it negotiates a contract but does not live up to it. Or an agent could use investigative powers, such as searching for information on certain individuals in a database, in which case an agent must identify itself to an agent platform in order to verify the authority of the agent. In all of these scenarios the ability to identify an agent (and its principal) is necessary.

In addition to identification, a process of authentication whereby the truthfulness and validity of an agent's identity are confirmed is necessary too. Authentication is needed to prevent rogue agents posing as other agents from entering an agent platform or accessing a database, or to verify whether an agent is still authorised to act on its principal's behalf. Authentication features can be implemented in software agent design amongst other ways using public

key cryptography. On the basis of the verified identity, the agent can be authorised to perform certain tasks on the agent platform.

2.10.4 Integrity

Integrity of data is an important element of computer science in general and this is also the case for agent technology. An agent and the multi-agent system in which it operates must be protected from unwanted alterations, caused either by system malfunctions or by malicious intent, if the agent is to operate in a proper and trustworthy fashion (Brazier *et al.* 2003, p. 58). When the integrity of an agent is compromised it might act differently from its normal way of acting and could even cause damage or harm to its principal and other parties. Such behaviour will undermine an agent's usefulness and trustworthiness and put its reputation and that of its principal at risk. Therefore, adequate safeguards for the integrity of individual agents and the agent systems in which they operate must be put in place.

2.11 Provisional conclusion

At the time of writing this thesis we are still in the first phase of the agent-technology development, in other words, in the phase of the use of closed agent systems. Though advances in the field of agent technology are rapid, I believe it will still take many years before we reach the stage of fully scalable agent systems able to handle near limitless amounts of highly intelligent agents. It is therefore likely that if agents are to have a large-scale impact on our society and the way in which surveillance is conducted, it will be somewhere in the medium-term future.

For now, the use of agent technology is limited to closed systems and relatively simple automation tasks. Still, as I shall demonstrate in the chapter on agent-enabled surveillance, more advanced applications are being considered.

3 Surveillance and control

Trust is good, control better.
Vladimir Ilyich Lenin

In this chapter I shall investigate the subject of surveillance. In section 3.1 I shall give a general description of the concept of surveillance and explain why surveillance actually has two faces. In section 3.2 I shall discuss the present day surveillance landscape (known as the surveillant assemblage). Section 3.3 will focus on electronic surveillance and section 3.4 will focus on the trend towards system integration. The effects of electronic surveillance and system integration (the Superpanopticon and the panoptic sort) will be discussed in section 3.5. In section 3.6 I shall reverse the idea of the Panopticon, and discuss the unseen Panopticon. In section 3.7 I shall discuss the use of synoptic surveillance as a possible means to restore the balance of power between the watchers and the watched. The chapter shall be concluded in section 3.8.

3.1 The two faces of surveillance

This thesis deals with the use of software agents for surveillance, a goal that carries a negative meaning for many people because of its potentially grim Orwellian implications. The idea of living in a total surveillance society like Oceania, portrayed in George Orwell's (1949) *Nineteen Eighty-Four*, instils fear in the hearts of the public, making people weary of any increase in surveillance practices. Surveillance -which literally means to watch over- is oftentimes regarded as a potential invasion of privacy and an encroachment upon human rights and civil liberties. Still, we find that despite these fears, surveillance is increasingly abundant in many aspects of modern life. This dichotomy between human instinct and everyday reality can be explained by the fact that surveillance actually has two faces (Lyon 2001, p. 3).

Surveillance is defined by Lyon (2001) as the collection and processing of personal data, whether identifiable or not, for the purpose of influencing or managing those, whose data have been garnered. We must take care not to oversimplify the issue of surveillance by viewing surveillance solely as a disciplinary tool. The primary stimulus for the rapid proliferation of surveillance in our everyday lives is not the need for social control, but rather

the changes in the institutional order of society (Lyon 2001, p. 3). Therefore, we must differentiate between two distinct types (or faces) of surveillance: *disciplinary surveillance* and *liberal surveillance* (Innes 2003, p. 115).

3.1.1 Disciplinary surveillance

Surveillance makes the exercise of power more efficient and effective. Therefore surveillance has traditionally been the province of the authorities. The ability to watch over their subjects provided those in power with the means to exercise a greater deal of control. Many accounts of surveillance activity can be found throughout history, examples are the Roman city life, the plague control in medieval Europe, the monitoring of the poor in colonial times, and the slave trading in America (Sennet 1990, Foucault 1975, Gilliom 2001, Parenti 2003).

Disciplinary surveillance involves the purposive monitoring of conduct to allow for the identification, acquisition, and classification of information with the intention of modifying that conduct in some manner (Innes 2003, p. 113). Surveillance in this sense is a mechanism for exercising social control. Cohen (1985) defines social control as those organised responses to crime, delinquency, and allied forms of deviant and/or socially problematic behaviour which are actually conceived of as such, whether in the reactive sense (after the putative act has taken place or the actor has been identified) or in the proactive sense (to prevent the act).

The idea of surveillance as a technology of power, rationalisation, and control can be attributed mainly to Foucault. In his seminal work *Discipline and Punish* Foucault (1975) described how in post modernity rational means of ordering society have in some way replaced traditional methods such as brutal public punishment (Lyon 1994, p. 7). One of the most important elements of these rational means is the extensive use of surveillance. According to Foucault surveillance can be used to induce in subjects a state of conscious and permanent visibility that ensures the automatic functioning of power. Surveillance instils discipline by forcing self-regulation of the subject (Parenti 2003). Foucault's analysis of surveillance and discipline still features prominently in the contemporary surveillance discourse, therefore we shall study his arguments somewhat more in depth in this subsection.

Panopticism is based on the belief that control over individuals is made possible through a system that facilitates the continuous, automatic, disciplinary surveillance of persons determined to be in need of correction or normalisation (Gandy 1993, p. 21). The ideas behind Panopticism were derived from Bentham's work by French philosopher Foucault (1975) in his influential work *Discipline and Punish: the Birth of the Prison*. In 1791, the social reformer and philosopher Bentham, introduced a new type of penitentiary design that he called the Panopticon, Greek for 'all-seeing place' (Bentham 1843). The architectural features of the Panopticon would induce in the inmates "a state

of conscious and permanent visibility that ensured the automatic functioning of power" (Foucault 1975, p. 201).

The architectural design of the Panopticon featured a central tower with an annular building at the periphery. The peripheric building was divided into cells that had two windows: one on the outside that allowed light to enter the cell and one on the inside to allow for permanent visibility of the inmate. The central tower housed the supervisor, who was hidden from the view of the prisoners through an intricate design of windows, shutters, and lighting. From the central tower the supervisor was continuously able to observe the inmates, or as Foucault (1975, p. 200) puts it:

> "By the effect of backlighting one can observe from the tower, standing out precisely against the light the small captive shadows in the cells of the periphery. They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualised and constantly visible."

The fact that the supervisor himself was not visible was one of the key elements of the Panoptic design. Bentham laid down the principle that power should be visible but unverifiable (Foucault 1975, p. 201). Power was clearly visible in the form of the outline of the central tower, but its exercise was unverifiable as a result of the window, shutter, and lighting design that rendered the supervisor invisible. Inmates were thus placed under the impression that the gaze of the supervisor was continuous and unrelenting. The Panoptic design ensured that the inmates did not know whether they were actually being watched, thus giving them the impression that they could be at any given time. This situation made obedience the only rational option for the inmate, as deviant behaviour was most likely to be noted by the supervisor (Lyon 1994, p. 63).

In a sense the Panoptic design shifted the exercise of power over to the side of the surface of its application (Foucault 1975, p. 202). Those who are subjected to a field of visibility and are aware of this situation automatically assume responsibility for the constraints of power and alter their behaviour to meet its demands (Foucault 1975, p. 203). In this way the watched actually subjugate themselves to the power of the watchers through a process of self-regulation. This also makes the actual exercise of power in the form of harsh (corporeal) punishment unnecessary in light of the fact that the subjects are "caught up in a power situation of which they themselves are the bearers" (Foucault 1975, p. 201).

The Panoptic model forms a break with previous technologies of power and discipline that relied primarily on force and violence exercised through the authority of sovereignty. Rather than the exercise of power through the right of the sword, Panopticism made the exercise of power lighter, more rapid, and ultimately more efficient and effective. Panopticism was "a design of subtle coercion for a society to come" (Foucault 1975, p. 209).

The Panopticon must be seen as a generic model for the functioning of power and discipline that can be detached from any specific use as well as its original architecture (Foucault 1975, p. 205). The Panoptic model can be used for disciplining individuals in any environment that can provide complete and unverifiable visibility of the subject. While in the past this meant the Panoptic model could only be successfully implemented within discrete institutions such as the prison, mental ward, or army barrack, it could be argued that the rise of surveillance technology now makes Panopticism feasible on a much larger scale, turning our entire society into what Poster (1990) has called the Superpanopticon. But before we turn our attention to electronic surveillance and its panoptic effects, I will describe liberal surveillance.

3.1.2 Liberal surveillance

Every society, from past to present, has evolved mechanisms for the observation of its members. Though historically mainly the province of the state, in our time surveillance is also routinely conducted by private entities. According to Lyon the rapid proliferation of surveillance practices can be attributed largely to changes in the order of our society. Surveillance is oftentimes a necessity due to the way we structure our political and economic relationships in a society that values mobility, speed, security, and consumer freedom (Lyon 2001, p. 3).

The advent of information and communication technology has led to a situation were social interaction has become increasingly 'disembodied' (Lyon 2001, p. 15), that is to say, conducted without the physical presence of both parties and possibly asynchronously. In order to restore the feeling of trust lost as a result of disembodied communication, a wide variety of surveillance methods have been developed and are currently being used by both public and private entities to identify and authenticate the opposing party.

In fact, without liberal surveillance many forms of interaction and communication would be impossible in the information society. For instance, it is necessary to keep records of telephone conversations for billing purposes.

Moreover, though surveillance provides ample opportunity for abuse, in general people seem to celebrate the arrival of many new surveillance methods. Most people are more than willing to comply with surveillance given the fact that most of the time it is conducted with a plausible justification and/or provides tangible benefits to those willing to be subjected to it.

An example of an in itself pervasive surveillance technology that is readily accepted is the use of Closed Circuit Television (CCTV) in public areas. Great faith is placed in the possibilities of this technology to curb crime, and indeed, people are willing to relinquish part of their privacy and anonymity for increased security. In this sense surveillance encapsulates a 'caring' sense of

watching over and assists in enhancing objective and subjective security (Innes 2003, p. 117).

In the private domain a good example is the use of customer loyalty programmes. Consumers allow companies to watch and record their shopping behaviour in exchange for benefits such as better service or lower prices.

The supposition that surveillance is solely a means of disciplining the subject is therefore too simplistic and must be rejected. However, we must not disregard the fact that liberal surveillance methods can also be employed for disciplinary purposes. I shall discuss this problem in the following sections.

3.2 THE SURVEILLANT ASSEMBLAGE

Since its conception in the late 1970s the Panoptic model has dominated the discussion on surveillance and society. However, developments of a social and technical nature have prompted scholars to rethink Foucault's classic theory. The spread of liberal surveillance in almost every aspect of modern life as a result of information and communication technology has led to a situation that Haggerty and Ericson (2000, p. 605) dubbed the 'surveillant assemblage'. They argue that Panopticism is too monolithic in its approach and disregards the developments with a social and a technological nature that have changed the surveillance landscape considerably.

An assemblage consists of a "multiplicity of heterogeneous objects, whose unity comes solely from the fact that these items function together, that they 'work' together as a functional unity" (Patton 1994, p. 158 as quoted in Haggerty and Ericson 2000). In other words, an assemblage is not a discretely bounded, structured, and stable whole, but is made up of a multitude of interrelated parts. Surveillance is driven by "the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole" (Haggerty and Ericson 2000, p. 610). In this sense surveillance is an assemblage of individual surveillance practices and technologies.

Haggerty and Ericson (2000, p. 614) describe surveillance as rhizomatic, a term derived from botany by Deleuze and Guattari (1987). A rhizome is a horizontal stem that grows outwards from a plant and sends out roots and shoots from its nodes, usually from underground. Examples of plants that have rhizomes are asparagus and weeds such as crabgrass or thistle. Rhizomes expand fast, have strong regenerative capabilities, and are difficult to destroy due to their 'distributed' nature. New offshoots can be formed at any point of the rhizome so they have no inherent hierarchical structure such as a tree, where offshoots branch off from the main stem and new branches from these initial offshoots. Modern surveillance is developing in much the same way as rhizomes, expanding fast and fragmentary throughout many different social arenas without a centralised, hierarchical structure. The result is a complex

set of layered and nested assemblages wherein previously discrete surveillance systems are becoming increasingly interlocked (Innes 2003, p. 126).

There is no single entity in control of all these systems, but rather control is distributed throughout a host of different actors in society. The individual practices and technologies are not limited to public parties but are also conducted by private parties. The surveillant assemblage model thus rejects the panoptic model that hints implicitly at a single controlling entity. As such the classic 'Big Brother' metaphor no longer accurately describes the current surveillance landscape.

But despite the fact that the 'Big Brother' metaphor is no longer completely accurate, this does not mean that the significance of state surveillance is any less. On the contrary, when the need arises the state can 'tap' into the private sector surveillance apparatus and obtain additional surveillance data. As such public sector and private sector surveillance is increasingly integrated (Lyon 2003b, p. 105).

3.3 Electronic surveillance

For its operation surveillance depends heavily on technology. In my opinion the increase in surveillance practices can be attributed largely to the rise of information and communication technologies. In a sense, information and communication technologies are both cause and effect of surveillance. On the one hand it has enabled people to conduct their interactions over a distance leading to a growing demand for surveillance. On the other hand technology has provided our society with the tools to realise goals such as security, convenience, efficiency, and risk management.

Information and communication technology plays a pivotal role in the process of rationalisation and control. Surveillance capabilities are for a large part aimed at the human body (Haggerty and Ericson 2000, p. 611). The body is broken up into a series of data flows that can be collected, stored, and analysed at will. With these data a 'data doppelganger' can be created that exists alongside the real person. The information that makes up an individual's data doppelganger can be retrieved from a variety of different sources both public and private. The accumulation and reassembly of data in the surveillant assemblage is facilitated by the integration of previously isolated surveillance systems.

3.4 System integration

As mentioned in the previous section, surveillance is driven by the desire to bring systems together and integrate them into a larger whole. While discrete surveillance systems may be effective in their operation, the integration of

multiple systems within the surveillant assemblage is likely to increase exponentially the effectiveness of surveillance. The ability to store, sort, classify, retrieve, and match information garnered from multiple surveillance systems is crucial to the effectiveness of surveillance (Norris and Armstrong 1999, p. 219). The abilities of individual surveillance systems are augmented when multiple systems are combined into a surveillance network. Individual bits of information with nominally limited uses are combined and thereby transformed into powerful tools for monitoring groups and individuals, a process known as 'function creep' (Parenti 2003, p. 85).

Function creep is possible because surveillance practices and current flows of data move much more freely between different settings than previously (Lyon 2001, p. 36). In the past the surveillance containers were relatively well sealed which meant that information garnered in one setting, rarely affected another surveillance setting. However, the surveillance containers are becoming increasingly leaky (Lyon 2001, p. 36). As a result data gathered in a liberal surveillance setting can still pose a potential risk to the privacy and individual liberty. The reason is that information gathered in the context of liberal surveillance can also be used for the purpose of disciplining and controlling individuals or groups.

Though system integration is a definite trend in surveillance, there are several socio-technical inhibitors, and practical limitations to the development of a fully functioning, all encompassing, surveillance network (Innes 2003, p. 126), namely *interoperability*, *inter-organisational cooperation*, and *legal barriers*.

Interoperability

The first limitation is *interoperability*, which in essence is of a technological nature. The surveillance systems to be integrated must be able to communicate with each other. To this end their infrastructures must be compatible and able to share information between one another. At present, most surveillance systems and the accompanying databases are 'stand-alone' systems. The next challenge here is semantic interoperability, in other words, surveillance systems based on different ontology's can still exchange relevant information that they do not misunderstand.

Currently, agent technology could speed up interoperability through the use of wrappers. A wrapper is an environment that functions as an intermediary between the surveillance system and software agents wanting to interface with the surveillance system. A wrapper can be built on top of existing legacy systems and accommodate for visiting software agents. Through the use of wrappers agent systems and other computer systems can be effectively integrated.

Inter-organisational cooperation

The second limitation is *inter-organisational cooperation;* which has to do with the inability or reluctance of organisations to share information with each other.

In particular, in the private domain the willingness to cooperate and integrate systems seems lacking between different organisations. Information is a valuable asset and not many companies are willing to share readily such a resource with other companies.

The lack of inter-organisational cooperation was one of the most important reasons the terrorist attacks on the World Trade Center and the Pentagon went unnoticed (Sawyer 2003). The various agencies within the Intelligence Community (most notably the FBI, the CIA, and the NSA) not only failed to share effectively information with each other, but also with state and local authorities (Graham *et al.* 2002, p. 354). As a result of the September 11, 2001 terror attacks, inter-organisational cooperation has become a key issue in strengthening the information position and effectiveness of the Intelligence Community (Kean *et al.* 2004, p. 416).

Legal barriers

The third limitation is the result of *legal barriers* that have been put in place to limit system integration. The law often prohibits the integration of surveillance systems and databases in order to prevent the concentration of power. It is my opinion that the first two barriers that are of a technological and organisational nature could be resolved in time. If this turns out to be the case, the law will be the only barrier remaining between the current situation and total system integration. What the possible consequences of total system integration might be will be the topic of the next section.

3.5 Superpanopticon and panoptic sort

In the previous sections we have established that the surveillance net is being cast wider while the meshes are becoming smaller. The expansion of both liberal and disciplinary surveillance practices is the result of a growing need for efficiency, security, risk management, and control. The ongoing development of new surveillance technologies and the trend towards system integration facilitate the emergence of a progressively more efficient system of control. Ultimately this could result in a society that is so permeated by the unrelenting gaze of surveillance that the society itself would become a giant Panopticon. Mechanisms for unobtrusive electronic monitoring combined with the ability to store, sort, classify, retrieve, and match (Norris and Armstrong 1999, p. 219) information could even surpass the level of effectiveness attained in Bentham's Panopticon. The latter observation has led Poster (1990) in an earlier stage to describe the workings of modern surveillance in society as 'Superpanoptic'.

3.5.1 Superpanopticon

The essence of surveillance according to Foucault is the accumulation of information and the direct supervision of subordinates (Lyon 1994, p. 66). In many cases Panopticism serves as the guiding principle for the application of modern surveillance technologies. The emergence of a Superpanopticon invokes strong images of a totalitarian rule and indeed the state apparatus could use the Superpanopticon to bring its disciplinary power into play. The surveillant assemblage is no guarantee against the risk of excessive state surveillance because individual systems are increasingly integrated (Lyon 2003b, p. 105). In this way information garnered in a liberal surveillance setting can be used for disciplinary purposes.

3.5.2 Panoptic sort

Although the excessive use of surveillance by the state remains a point of vigilance, another panoptic scenario also demands strong attention. The 'panoptic sort' is a name assigned by Gandy (1993, p. 15) to the complex technology that involves the collection and processing of information about individuals and groups that is generated through their daily lives as citizens, employees, and consumers. The information is used to coordinate and control their access to the goods and services that define life in the modern capitalist economy.

At the heart of the panoptic sort lies a process of *identification*, *classification*, and *assessment*. Together these three functions form an integrated procedure. The first step in the panoptic sort is identification. When a person presents himself at a particular time or place, he is identified by means of identifiers such as tokens (cards, forms), signatures, or biometric information. Identification allows for the authentication and authorisation of certain claims made by the individual, but also opens up the possibility of classification (Gandy 1993, p. 16). *Classification* involves the assignment of individuals to conceptual groups on the basis of identifying information (Gandy 1993, p. 16). The third and final function necessary for the operation of the panoptic sort is *assessment*, which is a comparative form of classification (Gandy 1993, p. 17). It is the process of assessment that determines whether individuals should be included or excluded when it comes to social and economic relations (distribution of goods, use of services).[1]

1 We may judge from this paragraph that information plays an important role in economic relationships. Another issue related to the panoptic sort is the influence information may have on the equality of parties in economic relationships. When one party has more information than the other party, a situation of 'economic inequality of arms' may arise (Van den Hoven 1999). One possible effect of this economic inequality of arms is price

Though Gandy (1993) limits his description of the workings of the panoptic sort to the area of the free market economy, I feel it is equally applicable to state surveillance, as state surveillance also works through the process of identification, classification, and assessment.

The intensity and effectiveness of the panoptic sort is for a large part determined by the power of digital surveillance technologies. Continuing advances in the field of surveillance technology will undoubtedly add to the already significant influence of the panoptic sort. As the mechanisms of the panoptic sort become more sophisticated the possibilities for abuse increase. When groups and individuals are judged on the basis of their personal information, surveillance turns into a mechanism of social sorting that could threaten social equality and cohesion (Lyon 2003a).

3.6 Reversal: the unseen Panopticon

Up until now I have discussed the Panopticon and the negative effects that it may have on privacy and (individual) liberty. The idea of the Panopticon is based upon the premises that an individual is aware that he is subjected to continuous scrutiny. This knowledge on the part of the individual is essential for the functioning of the Panopticon. However, in our modern information society it is oftentimes unclear when and how an individual is being watched. More often than not, people are unaware that they are being monitored by means of electronic surveillance. When it comes to unobtrusive monitoring through electronic surveillance, software agents are particularly well suited for this task.

So oftentimes, even though an extensive surveillance system is present, panoptic effects will not occur.[2] However, the absence of panoptic effects does not imply that there is no threat to privacy and individual liberty. In many aspects the fact that people are unaware of the fact that a powerful surveillance infrastructure is in place may be equally if not more harmful. The power

discrimination (see for instance: Odlyzko 2003). As the processing of (personal) data becomes progressively less expensive and more efficient, this issue will become greater. The right to privacy is a means to maintain economic equality of arms. However, given the subject matter of this thesis I shall exclude this issue from further discussion.

2 We can see this, for instance, in the monitoring of public places by means of CCTV. In general, people do not seem to be bothered by the presence of CCTV systems and do not behave differently as a result of it (Gill and Spriggs, 2005). In my opinion this can be explained through the fact that in general people experience the presence of CCTV as benevolent (i.e., it increases their sense of security). Whether (potential) criminals experience panoptic feelings is more difficult to establish. An indicator would be a decrease in crime in the areas surveilled by CCTV. However, it seems that the findings from studies into the effectiveness of CCTV are inconclusive (see for instance: Gill and Spriggs, 2005) on this point, and as such it is hard to establish whether (potential) criminals actually experience panoptic feelings.

derived from knowledge gathered through a powerful surveillance infrastructure can still be used to identify, classify, and assess people. Moreover, the information can even be used to influence or manipulate people without their knowledge.

The threats of the unseen Panopticon mentioned above require an active, and sometimes even malevolent approach on the part of the observers. It is my belief that while possible, these kinds of scenarios are not commonplace. However, the unseen Panopticon might also affect people in a different way, something that Solove (2004b) describes by introducing the 'Kafka metaphor' into surveillance theory:

> "I argue that the problem is best captured by Franz Kafka's depiction of bureaucracy in The Trial a more thoughtless process of bureaucratic indifference, arbitrary errors, and dehumanization, a world where people feel powerless and vulnerable, without any meaningful form of participation in the collection and use of their information."

What this quote illustrates is that the workings of the Panopticon are far less straightforward in the information society than in Bentham's Panopticon. While people might experience panoptic feelings (the classic Big Brother metaphor) as a result of electronic surveillance and the exchange of personal data between different actors in the surveillant assemblage, it is also likely that they will not, since it is oftentimes totally unclear to an individual who is collecting and processing their personal data.

3.7 SYNOPTIC SURVEILLANCE

The (super)panoptic model approaches surveillance first and foremost as a top-down phenomenon whereby the powerful few watch the less powerful many (Innes 2003, p. 126). The surveillant assemblage introduces the notion of decentralisation of surveillance technology, but the distribution of the surveillance technology (and thus power) is still in favour of those in a position of political or economical power. Ongoing system integration even (re)introduces panoptic elements into the surveillant assemblage.

However, there are clear signs that the gaze of surveillance is also being inverted, meaning that the watchers are now themselves being watched. Sociologist Mathiesen (1997) has contrasted the panoptic model with that of the 'Synopticon' where the many watch the few (Rosen 2004). The Synopticon, like electronic surveillance, is made possible by advances in information and communication technology. A good example of a technology that facilitates synoptic surveillance is television. Unlike other surveillance tools such as CCTV, television is not used to watch the general population, but rather the authorities. The most striking example is the incident involving police brutality against Rodney King that was captured by a video amateur. The recording

exposed the misconduct of the authorities and sparked violent riots in Los Angeles. Another example of synoptic surveillance is the *Cryptome Eyeball Series*, a website dedicated to watching those in power.[3]

Brin (1999) argues that synoptic surveillance could serve as a means to restore the balance of power disturbed by the panoptic use of surveillance. In his book the *Transparent Society* he advocates a form of 'reciprocal transparency' whereby all actors in society must be able to access surveillance powers. Brin argues that the current distribution of surveillance power in society is unequal as it is concentrated mainly within existing power structures like the government and the major corporations. In order to restore this balance we must not try to hide information or ban the use of it through the right to privacy, but rather we must opt for full transparency using a *quid pro quo* system of surveillance. When an actor in society (a person, government agency, or corporation) wants to bring surveillance powers to bear against another, the actor himself (or itself) must be submitted to the same form of surveillance. According to Brin this approach will stimulate the equal distribution of surveillance powers, increase transparency and accountability, and lead to a more responsible use of surveillance powers.

Brin (1999) puts forward a persuasive argument for reciprocal transparency that might prove to be a valuable alternative to invoking the right to privacy when it comes to surveillance. However, in its most extreme form, a society where any one can spy on one another, I feel Brin's transparent society is wholly undesirable, in view of the fact that it might lead to a tyranny of the majority over the few. A further problem with Brin's idea is also that it is almost impossible to distribute surveillance power equally amongst all. Surveillance is labour intensive and it is capital intensive, meaning most individuals cannot afford to use surveillance power in ways the more affluent individuals or institutions can.

Software agents might play a role in synoptic surveillance by helping individuals gather information about surveillance practices that are being employed against them. A software agent could for instance be used to effectuate an individual's right to participation. Article 12 of the European Data Protection Directive gives individuals the right to ask data controllers whether personal data about them is being processed. In practice, however, the right is seldom used, as most data subjects find it too difficult or tedious to gain access to their personal information, or are simply unaware of the existence of the right to participation.[4] For instance, a software agent could be used to automate this process for the data subject. This will increase transparency and add meaning to the right to participation.

---

3 http://eyeball-series.org/

4 See: The European Union Research Group, *Data Protection*, Special Eurobarometer no. 196, December 2003, p. 49.

3.8 PROVISIONAL CONCLUSIONS

Surveillance, in both a liberal and a disciplinary sense, is increasingly prolific in the information society. While historically mainly the province of the state, surveillance is now routinely conducted by both public and private parties as a result of changes in the institutional ordering of society and advances in technology. The idea of surveillance as a monolithic structure (along with the classic 'Big Brother' metaphor) is therefore more or less outdated. The current surveillance landscape can be most accurately described as a 'surveillant assemblage'.

In the information society individuals are being watched in such diverse settings as the workplace, the marketplace, and the public space. Consequently, the existence of many distributed, heterogeneous, surveillance systems is one of the key aspects of the surveillant assemblage. The data these systems generate is for the most part stored in searchable databases and while in general these systems are closed and discrete they can be integrated. The surveillant assemblage thus carries with it the realistic possibility of function creep.

Information and communication technology plays an important role in the integration of different surveillance systems. Amongst the technologies used for the integration of previously discrete systems, artificial intelligence (including agent technology) features prominently. In the next chapter I shall examine how agent technology is used to facilitate and integrate surveillance practices.

4 Surveillance and software agents

Sentient programs... ...they are the gatekeepers,
they are guarding all the doors, holding all the keys.
Morpheus, the Matrix

In this chapter I shall discuss how agent technology can be used to facilitate and integrate surveillance. The main goal of this chapter is to review the current state of the technology with regard to agent-enabled surveillance. This will allow us to determine the impact of agent-enabled surveillance on privacy and liberty and aid us in determining the adequacy of the current legal framework for the protection of privacy and liberty. I do not only want to examine the legal framework in the light of current technology in this thesis, but also view the legal framework in the light of possible future developments. Therefore, I shall also try to provide some insight into the possible future of agent-based surveillance.

I shall describe four applications of surveillance that benefit from agent technology *viz. knowledge discovery*, *data gathering*, *automated monitoring*, and *decision support*.[1] For each of these applications I shall give a description of how agent technology is implemented, explore applications that make up the current 'state of the art', and infer future developments based on the current implementation of agent technology. I shall explore knowledge discovery in section 4.1, data gathering in section 4.2, automated monitoring in section 4.3, and decision support in section 4.4. The findings will be summarised in section 4.5.

An important issue that will not discussed in the context of this chapter is who is responsible for the exercise of agent-enabled surveillance. This issue is important because the choices that are made with regards to the implementation of technology (i.e., what are the goals and the scope of agent-enabled surveillance) ultimately determine what impact the use of a particular technology may have on individuals and the society. However, since this is primarily a legal issue I shall discuss it in chapters 8 and 9.

---

1 In some cases, the areas of surveillance described and the accompanying examples display a certain overlap.

4.1 KNOWLEDGE DISCOVERY

Gathering and analysing data is vital when it comes to surveillance. Electronic surveillance, both in the disciplinary and liberal sense, typically generates large amounts of data. For the most part these data are stored in databases for future reference. As a result the amount of surveillance data available in countless disparate data sources worldwide is immense and growing at an exponential rate. Though these data might contain a wealth of knowledge, information overload and a lack of integration between databases make it hard to discover that knowledge. In order to enhance the effectiveness of surveillance, technologies for integrating databases and finding information contained therein are in increasing demand. The popular term for these technologies, while not entirely accurate, is data mining.

4.1.1 Implementation

Data mining is a technology whereby useful information is mined from large quantities of data, much like the process of extracting minerals from the earth. Over the past two decades it has evolved from an experimental technology into an important instrument to help overcome the problem of information overload. Data mining allows the automatic analysis of databases and the recognition of important trends and behavioural patterns (Ména 2004, p. 29).

A data mining exercise differs from a standard database query as it is aimed at finding previously unknown information in existing data. A standard database query returns information consisting of data from individual fields or records contained in the database (Taipale 2003, p. 22). The answer to a standard database query is always explicit, because it is a data item in the database. In addition, data mining is aimed at finding implicit information, such as patterns or relations in data, that were not previously identified and thus not themselves data items (Taipale 2003, p. 23).

While the term data mining is used to describe the entire process of knowledge discovery in databases, it is actually only a step in the process. The broader process of finding useful information in large quantities of data is known as knowledge discovery in databases (KDD). A definition of knowledge discovery in databases is: "the nontrivial extraction of implicit, previously unknown, and potentially useful information from data" (Frawley *et al.* 1992, p. 58). Still, data mining and knowledge discovery in databases have roughly become synonyms, with data mining being the most widely used term.

We can break the knowledge discovery process down into several distinct phases (Sietsma, Verbeek, Van den Herik 2002, p. 23).

1 Pre-processing
The first phase in the knowledge-discovery process is pre-processing. This stage involves steps such as goal definition, data collection, selection, and warehousing. When the goals of the data mining exercise have been defined the necessary data can be selected and collected. In traditional data mining, data collected from various sources is assembled into a single dataset that is stored in a data warehouse. The data-mining algorithms are applied to this data warehouse. But before the collected data can be mined effectively it must be cleansed, this means errors must be removed and missing fields must be completed.

2 Data mining
The actual data mining itself involves the application of particular algorithms to the data warehouse in order to elicit, identify, or discover certain previously unknown characteristics of the data, including descriptive and predictive patterns or relationships (Fayyad *et al*. 1996).

3 Post-processing
Post-processing consists of interpreting and evaluating the discovered patterns and determining their usefulness within the applicable domain context (Taipale 2003, p. 30). An important element of post-processing is determining to whom the results of the knowledge-discovery process should be addressed (Sietsma, Verbeek, Van den Herik 2002, p. 24).

Mining data from distributed sources
So far, we have discussed the classic data-mining process, but the classic, centralised data-mining approach described above is not always feasible. Advances in computing have resulted in countless heterogeneous and distributed data sources. Oftentimes the data in these data sources cannot be gathered into a single repository for processing due to privacy concerns, problems with scalability, or the fact that owners of the databases do not wish to share an entire dataset. Furthermore, the structure of these databases may differ and the data contained therein is not necessarily consistent. The field of distributed data mining (DDM) deals with this problem. In a distributed data-mining approach most of the processing takes place at the local database, with only aggregate data being sent to a central server.

Agent technology can play a key role in distributed data mining. In an agent-enabled distributed data-mining approach, software agents are sent to prepare and mine databases in different remote locations over open and closed networks (Ména 2004, p. 30). Software agents act as mediators between different data sources by providing logical and semantic interoperability. Furthermore, software agents can aid subject-based inquiries by removing the need for manually querying different data sources. In this approach the agent functions as a query broker and handler that can continuously, or at predefined

intervals, query remote data sources in (near) real-time without the presence of a human operator.

One way in which agents may perform such tasks is by associating with every database a database agent that is responsible for accessing the database and by associating with every client a client agent that is responsible for gathering the information requested by the client. These agents can provide the client with the requested information. The agents that make up a multi-agent system, collaborate in order to: (1) determine which agent can provide the requested information, (2) map a client's request onto database queries, (3) combine the information in such a way that the communication load is minimised, and (4) deal with inconsistencies among different databases.

Ontology's play an important role in a multi-agent systems. An ontology provides a formal specification of a shared conceptualisation. The ontology can therefore be used for producing a description of the knowledge stored in a database. Such a description is necessary to determine which database can provide which part of the requested information. Moreover, the ontology needed for specifying the database content, must be closely tied to the ontology used for communication and the ontology of the language in which the client formulates his/her request. (Van den Herik, Wiesman and Roos 2001)

The application of agent technology in the field of distributed data mining is in particular considered for the purposes of homeland security and anti-terrorism (Baird *et al.* 2003, p. 23). But the private sector also employs (distributed) data mining for purposes such as risk management and market research.

Taipale (2003) distinguishes between three discrete applications for automated analysis of data in the context of domestic security. The first application is *subject-oriented link analysis* where data mining is used to learn more about a particular data subject, its relationships, associations, and actions. The second application is *pattern analysis*, whereby a descriptive or predictive model is developed based on previously discovered patterns. The third application is *pattern matching*, whereby a predictive or descriptive model is used against new data in order to identify related data subjects such as people, places, relationships *et cetera* (Taipale 2003, p. 34). In other words data mining can be used to conduct either *subject-based inquiries* or *pattern-based inquiries*. These different types of inquiries influence privacy and individual liberty in different ways, so I shall discuss them separately. But first I shall elaborate on the value of data mining for law enforcement and anti-terrorism purposes.

In the surveillant assemblage personal data regarding individuals can be obtained from a variety, of public and private-sector databases. Agent technology presents ample opportunity for aggregating and integrating information across a variety of heterogeneous and disparate data sources. The power of data aggregation and integration within the surveillant assemblage was clearly shown in the investigation that followed the September 11 terrorist attacks. Within a few days an accurate record of the last days of Mohammed Atta, the alleged ringleader of the September 11 hijackers, was compiled from data

gathered from public, put predominantly private sector surveillance systems. The data included CCTV footage, credit card receipts, cell phone information, and airline tickets. Of course, since the information on Mohammed Atta was garnered *ex post* it was of no value in preventing the terrorist attacks. Had the information of these different surveillance systems been aggregated and integrated *ex ante* it might have led to the discovery of Atta's plans. This is the idea behind 'connecting the dots' and the driving force behind the wish to integrate surveillance systems. As described earlier, connecting the dots is perceived as vital when it comes to combating terrorism and other forms of serious crime. However, intensive aggregation and integration of data also poses a potential risk to privacy and individual liberty.

Subject-based inquiries
A subject-based inquiry is aimed at gaining a more complete picture of a specified data subject (for instance an individual or an organisation). Through a subject-based inquiry additional information regarding a particularised subject such as links, associations, history, and actions can be distilled from the available data.

Pattern-based inquiries
A pattern-based inquiry is a non-particularised search, that is to say, it is not aimed at a particular data subject or data subjects. By mining data in a non-particularised fashion, previously undiscovered relationships between individual data items can be discovered. *Pattern analysis* may aid law enforcement agencies and the intelligence community in developing descriptive or predictive models of deviant behaviour. A pattern-based inquiry can be used to develop a descriptive model or predictive model based on discovered patterns in existing data (pattern analysis or data mining in a narrow sense). Once a descriptive or predictive model has been developed it can be applied to new data in order to find similar or related data subjects (pattern matching).

The general idea is that the planning and organisation of a terrorist attack (or for that matter any crime that requires sufficient organisation) leaves behind a trail in surveillance data that makes up a distinctive pattern. By matching a discovered pattern to a new data set, suspicious behaviour not previously apparent can be found. By matching the predictive or descriptive model against new data similar patterns can be detected in an earlier stage, thus enabling a more pro-active method of investigation.

4.1.2 Current examples

Data mining is used extensively throughout society. The use of data mining does not restrict itself to the private sector but is also prolific in the public sector. For instance, a survey conducted in 2004 by the Government Account-

ability Office of the United States under 128 federal departments showed that 52 agencies were using or were planning to use data mining. These departments and agencies reported 199 data-mining efforts, of which 68 were planned and 131 were operational, some of which involved the processing of personal data (GAO Report 04-548). Though data mining was used for law enforcement purposes well before September 11, 2001, the terrorist attacks have definitely acted as a catalyst for the development of data mining in the area of law enforcement and homeland security. I shall restrict myself to giving examples of agent-enabled data-mining applications that are used for these purposes.

COPLINK[2]

COPLINK is a good example of how an agent-enabled data-mining application can make law enforcement more efficient and effective. COPLINK is a system used by law enforcement agencies in the United States to aid in criminal investigations. The COPLINK system was developed to provide a solution to the lack of integration in law enforcement information systems. COPLINK software organises and analyses vast quantities of structured and seemingly unrelated data, housed in various incompatible databases and record management systems, over an intranet-based platform (Knowledge Computing Corporation 2004). COPLINK integrates different data sources and facilitates subject-based inquiries.

Apart from integrating disparate databases COPLINK uses a collaboration and notification tool called 'Active Agent'. This component of the COPLINK system is a tool that can be set to watch for new data meeting user-specified parameters and then automatically notify the user(s) when such data is migrated into COPLINK (Knowledge Computing Corporation 2004). The COPLINK Active Agent thus automates the task of running repetitive or periodic database queries. The Active Agent also allows an investigator to collaborate with others who are conducting similar queries. If collaboration is set as active, the agent notifies other investigators running similar queries. This can quickly bring together incidents involving the same suspect or other database objects that are under investigation by different investigators, or by different jurisdictions (Knowledge Computing Corporation 2004).

InferAgent[3]

While COPLINK is designed specifically for law enforcement purposes, many commercial parties also provide 'off the shelf' data-mining solutions that can be used for law enforcement and homeland security. One such program is InferX Software's *InferAgent*. The *InferAgent* software suite uses agent technology to look for patterns and behaviours in networks made up of disparate databases. The agent technology used by InferX allows for (1) the automatic

2 <http://www.coplink.net>
3 <http://www.inferx.com>

analysis of separate, unlinked databases, (2) the recognition of important trends, and (3) behavioural patterns. These trends and behaviour patterns may identify suspicious activities and events related to fraud, terrorism, and theft. As conditions change in remote databases the InferX software agents detect the changes around them collaborating their findings to a centralised controller allowing for the discovery of potential threats, fraud, and risks.

ANITA[4]

In the area of subject-based inquiries, the ANITA project being conducted by research groups from the universities of Groningen, Utrecht, Maastricht, and Leiden is of particular interest. The ANITA project aims to design an agent framework wherein administrative agents will decide, based on norms, whether to allow transactions of police data.

Currently, the information infrastructure of the Dutch police does not allow for complicated search queries in the police registries that deal with serious forms of crime. Agent technology can provide a solution to this problem (Koelewijn and Kielman 2006). By setting up a national registry on serious crime (beheersindex) that is only accessible to software agents, a fast and flexible query system is created. Privacy risks are avoided since humans have no access to the system and the software agents that have access to the system base their behaviour on pre-determined rules.

4.1.3 Future

The inability of the intelligence community to predict and prevent the September 11 terrorist attacks underlined the importance of the ability to 'connect the dots' when it comes to (surveillance) data. Judging from the amount of data mining applications currently being considered, developed, and deployed, a great deal of faith is placed in data mining to ensure security. Whether this faith is justified remains subject of debate, but as the 'war on terrorism' goes on, the drive towards more effective ways to integrate databases is likely to continue.

It is important to recognise the importance of the surveillant assemblage when it comes to the future of data mining. Governments, most notably the United States government, actively pursue ways to use data contained in private-sector databases for public purposes, such as law enforcement and homeland security. The most prominent evidence to this intention is the DARPA's Total Information Awareness initiative. Although the Total Information Awareness programme was discontinued, it did offer us a glimpse into the (planned) future of data mining. Two proposed programmes, the *electronic*

4 Administrative Normative Information Transaction Agents (ANITA), NWO/ToKeN project no. 634.000.017.

evidence and link discovery (EELD) programme and the GENISYS programme were aimed at bringing data mining to the next level. Of these two programmes the GENISYS programme is most relevant to the subject matter of this thesis, for it would use agent technology as a primary tool for integrating disparate databases.

The GENISYS programme, sought to produce technology for integrating and broadening databases and other information sources to support effective intelligence analysis aimed at preventing terrorist attacks on the citizens, institutions, and property of the United States (DARPA 2003, p. 5). The technology to be developed would enable many physically disparate heterogeneous databases to be queried as if they were one logical 'virtually' centralised database (DARPA 2003, p. A-11). GENISYS was discontinued in September 2003 along with the other programmes that made up the Total Information Awareness programme. Still, it is interesting to study the GENISYS programme more in depth as it a prime example of the use of software agents for distributed data mining.

GENISYS would address the problems of current database technologies, which have their roots in the mid 1970s. In a time when process power, disk space, and bandwidth were expensive, time and space efficiencies were stressed at the expense of flexibility and ease of use, making automation a difficult task. Furthermore, human operators using a database have to know a great deal about the design of a particular database (for instance, how data items compare to real-world objects or people) in order to make sense of the data contained therein (Dyer 2003). An additional problem is the fact that database design differs from database to database, hampering effective integration.

In order to overcome these problems GENISYS was aimed at achieving three separate but related goals. The first goal was to enable the integration and restructuring of existing legacy databases. The second goal was to increase the coverage of vital information by making it easy to create new databases and attach new information feeds automatically. The third and final goal was to create a brand new database technology based on simple, scalable, distributed information stores known as repositories (Dyer 2003).

One of the technologies driving GENISYS would be software-agent mediation. Software agents would relieve human analysts of the difficult tasks of having to know (1) all the details about how to access different databases, (2) the precise definition of terms, (3) the internal structure of the database, (4) how to join information from different sources, and (5) how to optimise queries for performance. Instead, this information would be encoded and managed by software agents (DARPA 2003, p. A-11). In this way mediation agents would provide logical and semantic interoperability of previously disparate data sources.

DARPA's data-mining efforts within the TIA programme anticipated the further evolution of information and communication technology, a development characterised by a trend towards ubiquity, interconnection, intelligence,

delegation, and human-orientation that will continue well into the future. These trends will eventually culminate in the next ICT paradigm, that of ambient intelligence (Ahola 2001). In a world where we are surrounded by ubiquitous computing and intelligence no single part of our lives will per default be able to seclude itself from digitisation (Langheinrich 2001).

Since the data generated by our intelligent environment will dwarf current volumes of data, automated and intelligent processing of data is a prerequisite for effective surveillance. For example, it is estimated that the EPCglobal Network, a worldwide Radio Frequency Identification (RFID) network for tracking and tracing fast moving consumer goods, will generate terabytes (if not petabytes) of data on a daily basis.[5] Without the technology to interpret these data they are useless. Software agents and other artificial-intelligence technologies are needed to process the enormous amounts of data and make sense of the information contained therein.

4.2 DATA GATHERING

Data is not only stored in databases. The internet, i.e., the worldwide system of interconnected computer networks, is also host to a vast amount and a large diversity of data. These data are either stored on servers in order to make them publicly available (webpages, newsgroups, peer-to-peer networks), or generated in the course of communication between different actors (email, Voice over IP, Internet Relay Chat).[6]

The internet is not only used by law-abiding citizens, but also by criminals and extremists. One of the main reasons criminals and extremists use the internet is that it provides easy and secure communication. Moreover, the internet is used as a 'propaganda tool', for instance, to draw new recruits into the Islamic Jihad (AIVD 2004, p. 29). At this instance we see that the problem of information overload is especially apparent on the internet. The sheer size of the internet and the fact that most data on the internet is in unstructured form (i.e., natural language) means searching for information that suggests illegal conduct is a daunting task. Therefore, tools are created that can cope with the problem of information overload on the internet.

---

5 http://www.epcglobalinc.org

6 From a legal point of view, it is important to distinguish between these different types of information, because the applicable privacy-protection regime is in part dependent on the mode of communication. For instance, the privacy protection of email communication is stronger than that of information made publicly available on a website.

4.2.1 Implementation

Software agents are frequently used on the internet. All sorts of spiders, crawlers, and softbots are used to extract useful information from the internet. In general, these systems are not very intelligent and do not possess much autonomy and authority, but as technology advances it is to be expected that more intelligent and capable systems will be developed.

The dominant mode of retrieving information from the internet is the search engine. In general, an internet search engine works by storing indexed information about webpages (and possibly newsgroups) in a database that can be accessed by users. When a user presents a query to the search engine it looks up the index and provides a listing of best-matching webpages. Search engines use various techniques for determining the relevance, usefulness, or authority of a webpage. Apart from the normal search engines there are also meta-search engines. Meta-search engines act as an intermediary between the user and multiple search engines. Meta-search engines forward user requests to different search engines and present the results from each individual search engine to the user within a single user interface. By searching multiple search engines simultaneously more of the internet can be searched in less time.

Search engines and meta-search engines have proved to be important tools in countering the information overload. However, there are drawbacks to using (meta-)search engines; the most significant ones are (1) the need to fill in keywords manually, (2) the inability to discover patterns and associations between different pages or documents, and (3) the difficulty in finding worthwhile information based on a few keywords.

Apart from the ability to query multiple search engines in much the same way as meta-search engines do, software agents can provide added intelligence and personalisation to the information retrieval process. A software agent could, for instance, automatically track and report new search results or changes to existing search results (i.e., updated pages), collaborate with other information-retrieval agents, cluster and organise search results, pro-actively look for information based on a predefined user profile, and even retrieve information relevant to the environment of the user (Rhodes and Maes 2000). To this end agents employ artificial-intelligence techniques, such as fuzzy logic, case-based reasoning, and evolutionary computing (Mohammadian and Jentzsch 2004, p. 21).

4.2.2 Current examples

There are many examples of search engines that use agent technology to enhance search results. Below I will give an example of a commercial agent-enabled search-engine technology and a web mining application.

Tryllian ePosit
ePosit, an application developed by the Dutch company Tryllian, is an ASP application that continuously searches the internet for information deemed relevant by the user.[7] The documents that are of interest are stored in a database (the Documentbase) that can later be searched by humans. Documents can also be added manually, further expanding the Documentbase. The *ePosit* application relieves humans of the difficult and monotonous task of manually searching the internet, while providing them with an easy and structured way of finding relevant information.

XENON
In December 2004 the Dutch Tax Authority (Belastingdienst) started using a monitoring application named XENON.[8] The system, developed by Dutch companies Sentient Information Systems and Parabots, can be best described as a self-learning 'super' search engine. The system uses a combination of web-crawling technology and text analysis to patrol continuously the internet in search for businesses that are hidden from the view of the Tax Authority by conducting their economic activities online. Moreover, it is used by the FIOD/ECD and Customs Office to search for illegal goods, such as illegal fireworks and fake brand clothing.

4.2.3 Future

Currently, data gathering is for the most part limited to keyword searches. But as technology advances computers will gradually gain better understanding of natural language, greatly enhancing their surveillance capabilities. As of yet computer programs do not possess full natural-language understanding and therefore have problems grasping the meaning of the data available on the internet. It is thus difficult for a computer program to extract automatically concepts and relations in order to do query answering, inference, and other tasks. The subfield of artificial-intelligence known as *natural-language processing* (or text mining) aims at extracting useful information from unstructured or semi-structured text.

A second important development with regard to the retrieval of information from the internet is the *semantic web*. The semantic web is a development aimed at creating a common framework that allows data to be shared and reused across application, enterprise, and community boundaries.[9] So while natural language processing aims at extracting information from unstructured data on the internet, the semantic web is aimed at providing more structure to the

7 http://www.tryllian.com
8 http://www.sentient.nl; http://www.parabots.nl
9 http://www.w3.org/2001/sw/

data itself. The semantic web uses several different technologies, such as RDF (Resource Description Framework), OWL (Web Ontology Language), and XML (eXtensible Markup Language) to provide machine-understandable data on the web.

The development of natural-language processing and the semantic web will make information on the internet more readily accessible to software agents, further expanding their surveillance capabilities. It is thus to be expected that in the near future software agents will be far more capable at retrieving information from the internet. Consequently, the internet will likely become a more transparent place in the future.

4.3 AUTOMATED MONITORING

The use of surveillance cameras, also known as Closed Circuit Television surveillance (CCTV) is widespread throughout society. The permanent gaze of surveillance cameras can be felt in public transport, in buildings, and on the corners of many streets. It is estimated that in the United Kingdom alone, some 4,000,000 cameras monitor the public space.

While CCTV provides a vigilant eye in our physical world, technologies are also being developed that enable the intelligence community and law enforcement agencies to monitor the virtual world. In particular the internet is getting increasing attention from law enforcement agencies and the intelligence community. As was mentioned in the previous section the internet is a valuable communication tool for criminals, extremists, and even terrorists. For instance, according to a report issued by the Dutch secret service (Algemene Inlichtingen- en Veiligheidsdienst) the internet plays a significant role in the radicalisation of young Muslims (AIVD 2004, p. 44). Internet Relay Chat (IRC), for instance, is used by young Muslims to chat with like-minded believers and spiritual leaders. Chatting with like-minded believers can lead to a situation where young Muslims spur each other on towards increasingly radical ideas, a process called 'autonomous radicalisation' (AIVD 2004, p. 44). Surveillance technology could be used to notice the early signs of autonomous radicalisation and thus alert investigators in an early stage.

Here we may conclude that automated monitoring is seen as an important tool to help combat crime and prevent terrorism. With the advances in artificial-intelligence technology automated monitoring can be made more effective. In section 4.4 I shall describe how software agents can contribute to the effectiveness of automated monitoring.

4.3.1 Implementation

Up until now we have discussed how artificial-intelligence technologies, such as software agents can help retrieve explicit and implicit information from existing data sources. But agent technology can also be used in a more pro-active fashion. One area where agent technology can be used pro-actively is automated monitoring. Currently, predominantly human operators do monitoring tasks. But the limits of the human brain make it difficult for human operators to monitor behaviour effectively. The three main limitations of the human brain when it comes to surveillance are: (1) limited information intake, (2) limited attention span, and (3) limited ability for structuring data. Software agents can be used to overcome these limitations and thus provide a valuable alternative to human operators. Software agents can continuously monitor a given environment such as the public space or the internet and alert the user when suspicious behaviour is detected.

When we look at monitoring in the physical world we see that camera surveillance is the dominant mode of surveillance. In general a surveillance camera infrastructure is made up of multiple cameras. Software agents can be used to integrate the data from different cameras and present them to a human operator in a more comprehensible form, making the human operator more effective. Apart from integrating surveillance camera infrastructures, software agents can also add intelligence to the monitoring process. Software agents could, for instance, link camera footage to a database through the use of biometrics.

In the virtual world, agent technology is also used for automated monitoring tasks. Especially in the area of employee surveillance, software agents and programs that use agent technology are used. Typically, this type of surveillance is limited to a single network. However, more ambitious projects in the field of automated monitoring are being explored as I shall show in the examples.

4.3.2 Current examples

In this section I shall give two examples of how monitoring can be automated through agent technology. I shall give one example of automated monitoring in the public space and one example of the automated monitoring on the internet.

Combat Zones that See

In 2004 DARPA issued a call for proposals for an advanced research project titled *Combat Zones that See*. The goal of the project is to explore concepts, develop algorithms, and deliver systems for utilising large numbers (thousands) of cameras to provide the close-in sensing demanded for military opera-

tions in urban terrain (MOUT). While it is at this point uncertain whether software agents will actually be employed in the *Combat Zones that See* programme, a role for agent technology is likely.

The use of extensive surveillance networks is deemed necessary since the United States army is increasingly involved in asymmetric conflicts with cities and villages as battleground. Cities provide ample hiding places for combatants negating the superior situational awareness (provided by airborne reconnaissance) US combat personnel normally enjoy. Furthermore, collateral damage to civilians and buildings prevent the use of overwhelming force. As such, the make up of terrain prevents the United States army from capitalising on its strong points (superior situational awareness and stand-off firing capability), while enemies can use their superior knowledge of the terrain to their advantage. The hostage snatch mission in Mogadishu (1993) that resulted in the loss of eighteen US soldiers and ultimately led to the retreat of the United States from Somalia made this terribly clear (Edwards 1999, p. 52).

Automatic video surveillance and understanding will reduce the manpower needed to view and manage the collection of data. According to DARPA (Strat and Welby 2004, p. 6) the project will "assemble the video understanding, motion pattern analysis, and sensing strategies into coherent systems suited to Urban Combat and Force Protection." However, it is likely that the results from the project will also be implemented in surveillance projects for homeland security.

Piespy

Piespy is an application that can scan IRC channels. The program uses the data gathered to determine what relationships exist between chatters and can help infer social networks form this information (Mutton 2004).[10] An IRC bot (a rudimentary software agent) is used to monitor a channel and perform a heuristic analysis of events to create a mathematical approximation of the social network. From this, the bot can produce a visualisation of the inferred social network on demand. These visualisations reveal the structure of the social network, highlight the connectivity and cluster the strengths of relationships between users. Since *Piespy* can offer insight into the relationships of any type of social network, it could also be used to infer relationships between people suspected of deviant behaviour.

4.3.3 Future

In general, there is a strong drive towards more efficient ways to conduct surveillance and exercise control. As technology advances the ability to monitor

10 http://www.jibble.org

the physical and virtual world will become greater. Evidence of this development can be easily found in the areas of data mining, data gathering, and also in the area of automated monitoring. In this subsection I shall describe some possible future developments in the field of automated monitoring.

The public space

The ambient-intelligence paradigm plays an important role in the development of a more complete surveillance infrastructure through automated monitoring. The next step in the evolution of monitoring is the use of different types of sensors. Currently, the only type of sensor used extensively for surveillance tasks is the CCTV camera. In the near future the observing gaze will be augmented by microphones, motion detectors, heat sensors, *et cetera*.

Futurists are already exploring the concept of the 'ubiquitous city', an idea that ties in closely with ambient intelligence. In this vision of the future sensors and network technology will pervade the public space. By linking sensors with so-called 'locative media' such as GPS, RFID, and GIS, both people and objects can be tracked and identified throughout the public space. This will make surveillance far more effective. Though the concept of the ubiquitous city might seem far-fetched, pilot projects are already underway in cities like Osaka and Busan.

Software agents will play a key role in realising ideas such as ambient intelligence and the ubiquitous city. Software agents are needed to integrate the different sensors in a sensor network. Typically, sensor readings will generate huge amounts of data. These raw data need to be processed in order to distil useful information and knowledge. Currently, a centralised approach in processing data is most common, but such an approach places a large amount of stress on available network bandwidth since data needs to be transported from the distributed locations of the individual sensors to a centralised processing unit. Sensor networks currently being deployed already demand significant bandwidth (Brown and Wiggers, 2005). It is therefore likely that the centralised approach will not remain the dominant approach for long. Agent technology provides an alternative to the centralised approach by processing data at the source (i.e., at the sensor nodes) relieving pressure on the network.

The internet

In general, we can determine that automated monitoring of the internet will become increasingly advanced. But instead of further detailing gradual advances in internet monitoring, I have chosen to describe a more advanced application of agent technology that we might see in the future.

If artificial intelligence ever succeeds at approaching, equalling, or surpassing human intelligence, the possibilities for using software agents are seemingly endless. But while artificial-intelligence constructs, such as software agents, are far away from passing the Turing test, remarkable advances have

been made in emulating human intelligence, opening up the possibility for interesting law enforcement applications.

For instance, human-interaction software agents known as chatterbots, already engage in conversation with humans over the web and via instant-messaging services like MSN and AOL IM. These programs do not only engage in meaningless chatter, but also prompt human actors to buy products or visit particular websites. While these applications of agent technology are still fairly crude they do offer us a glimpse into the future.

By taking the chatterbot idea one step further, one could envisage an intelligent undercover software agent that engages in conversation with persons suspected of deviant behaviour. The undercover software agent could for instance infiltrate child pornography networks or terrorist cells. Undercover software agents could carry some of the workload and alleviate the pressure on human operators. Therefore, the idea of these kinds of software agents is pursued worldwide. As of yet, the application undercover software agents only exist in theory. Chatterbots are still a long way from passing the Turing test and are therefore unable to keep up an undercover appearance. However, in 2004 an article in *New Scientist* suggested differently.[11] John Wightman, a computer engineer from Schotland, claimed he had created a system known as *Chatnannies* that hosted 25,000 convincing chatterbots on a single agent platform that could unmask paedophiles.[12]

As minors frequent chatrooms predominantly, paedophiles use chatrooms to set up appointments with minors. The presence of paedophiles in chatrooms has alerted law enforcement agencies as well as vigilante organisations wanting to unmask paedophiles. Both law enforcement officers and civilians pose as minors on the internet in order to draw out and unmask paedophiles.[13] But monitoring chatrooms and engaging in conversations with paedohiles is a time-consuming task. Therefore scientists are trying to come up with ways to automate the process. Wightman claimed to have single-handedly succeeded in this task by building a convincing chatterbot that was able to pass the Turing test. Naturally, his claims were met with a great deal of scepticism from the AI community, who have been unable to come up with artificial-intelligence techniques able to pass the Turing test. Wightman has refused to let anyone test or examine the system. Though further research is needed before any significant conclusions can be drawn, it seems highly unlikely that Wightman's claims are authentic. Until Wightman gives conclusive evidence, we might safely assume that *Chatnannies* is a hoax. But whatever the credibility of the *Chatnannies* system, it serves as a good way to illustrate the way of thinking about how agent technology is developing.

---

11 *New Scientist,* web edition 6.4.2004.

12 I use the past tense because up until now no working prototype of the Chatnannies system has been delivered since it was announced in 2004.

13 See for instance: http://www.perverted-justice.com

4.4 DECISION SUPPORT

Automated monitoring can to some extent relieve human operators of the task of continuously monitoring the public space and the internet. But it is ultimately a human who must make a decision based on surveillance data regardless of the fact that they are gathered manually or in an automated way. Here the problem of information overload is also apparent: when there is too much information available on which to base a decision, the wrong decision could well be made. Therefore, decision-support systems are being developed that help human operators cope with the information overload. These systems filter, fuse, and integrate data and make the information more comprehensible by displaying it in a structured and easily accessible form. Though closely related to automated monitoring, decision-support systems are actually one step beyond automated monitoring as they are also able to assist human operators in making decisions.

4.4.1 Implementation

Decision-support systems are used extensively throughout our society and have been around for quite some while. Presently, we are in the first stages of developing more sophisticated decision-support systems known as (agent-based) collaborative decision-support systems. These systems are at the cutting edge of artificial-intelligence research and are being developed for complex, data-intensive applications. Agent-based collaborative decision support is a methodology utilising domain-specific intelligence systems to partner with human decision makers to reach a consensus solution to a complex problem (Sena 2000). The idea of an integrated, collaborative network of human actors and software agents working towards a common goal is particularly useful in chaotic and dynamic environments where the dependence on accurate and timely information is crucial.

An area where information is of crucial importance is the battlefield. The capability of a military force to create and leverage an information advantage will for a large part determine its combat strength. The idea of *network-centric warfare* is based on this premise. The term network-centric warfare broadly describes the combination of strategies, emerging tactics, techniques, procedures, and organisations that a fully or even a partially networked force can use to create a decisive warfighting advantage. Network Centric Warfare aims at utilising the power of information and communication technology for the more efficient and effective execution of military operations. Among the techniques used within the network-centric warfare concept are the so-called C4ISR systems, short for *Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance*. These systems use a combination of

information and communication technologies to facilitate surveillance and help human operators in their command and control tasks.

The military is a driving force behind the development of C4ISR systems, some of which are collaborative decision-support systems. Companies, such as BAE Systems, 21st Century Systems, and Global Infotek, are developing multi-agent systems for the United States military that are able to collect sensor data from distributed sources, fuse, and integrate these data, and present the information in a structured and easily accessible form to the human operator.[14] These interactive, flexible, and adaptable systems are developed for supporting the solution of a non-structured management problem for improved decision making. They utilise data, provide an easy-to-use interface, and allow for the decision maker's own insights (Turban 1995).

While at present the focus of C4ISR and collaborative decision-support systems is mainly on improving situational awareness on the battlefield, we can establish that these systems are also used outside the military. Mainly in the area of crisis management, companies and research institutions, such as Bull, Thales, Almende and DECIS lab are working on (agent-based) decision-support systems.[15] Moreover, recent interest in homeland security has led to an increase in the development of these kinds of decision-support systems that help counter asymmetric threats such as terrorism. It is therefore likely that the use of decision-support systems for surveillance and control tasks will increase over the coming years.

4.4.2 Current examples

Below three examples of collaborative decision support systems are given. While these systems do not feature surveillance as goals in themselves, but rather focus on decision support, they do illustrate the capacity for more effective control embodied in agent-based collaborative decision support systems.

COORDINATORS

The COORDINATORS programme is a DARPA sponsored effort to create distributed, intelligent software systems for automated decision support of military field units. The COORDINATORS system will help field units adapt their mission plans as the situation around them changes and impacts their plans. The COORDINATORS software does this by reasoning about the tasks assigned to a given unit, the task timings, how the tasks interact with those of other units,

14 http://www.alphatech.com; http://www.21csi.com; http://www.globalinfotek.com

15 http://www.bull.com; http://www.thalesgroup.com; http://www.almende.com; http://www.decis.nl

and by evaluating possible changes such as changing task timings, task assignments, or selecting from pre-planned contingencies.[16]

In this way COORDINATORS will take over some of the tasks that normally would be carried out by human users, and aid units in making battlefield decisions. Among the tasks that would be handled by COORDINATORS are information exchange, reasoning about the implications of change, option generation, and option evaluation. This will free up time for the human user to focus on more important tasks and will enable the human user to respond more quickly to changes on the battlefield. It is the ambition of the COORDINATORS program to create a system that over time will be able to learn to make decisions for the human user when he is occupied with other tasks.

COMBINED Systems

The COMBINED Systems programme, short for *Chaotic Open world Multi-agent Based Intelligently Networked Decision Support Systems*, is aimed at creating scalable multi-agent systems that help human decision makers cope with the chaotic and dynamic situations that arise in crisis situations. These multi-agent systems are able to create scalable *ad hoc* networks wherein agents and humans collaborate in order to reach better decisions in a crisis situation. The COMBINED Systems programme is being carried out by the DECIS lab; a joint venture of Delft University of Technology, Thales Nederland BV, TNO, Acklin, the University of Amsterdam, and the Maastricht University. Currently, work is being done on a validation scenario that involves a disaster in the Port of Rotterdam.[17]

Cybernetic Incident Management (CIM)

The CIM project is carried out by Dutch company Almende in association with the Delft University of Technology, the Vrije Universiteit Amsterdam, the Centre for Mathematics and Computer Science, Cmotions, and Falck. Its goal is to create a continuously adapting system that encompasses both people and supporting software and that has the ability to process and assess information in an adaptive, interactive, and intelligent fashion to support human decisions. The system will use software agents distributed throughout the network that are able to obtain and weigh information dynamically. As the system is self-learning, experience gained from simulations as well as real crises does not only reside in humans, but also in the software agents.

16 http://www.darpa.mil/ipto/programs/coordinators/index.htm
17 http://combined.decis.nl/tiki-index.php

4.4.3 Future

It is my belief that while at present surveillance applications such as data mining, data gathering, and automated monitoring are used in isolation, they will eventually merge into more comprehensive and integrated surveillance systems that have a strong focus on automation and (collaborative) decision support. Technologies such as RFID, sensor networks, data mining, and wireless networking, provide the building blocks to create large surveillance infrastructures that encompass both the physical and the virtual world. Within these infrastructures software agents will be used to perform all manner of functions. Besides providing a solution to technical problems such as bandwidth and load balancing, they will work in close conjunction with human operators enhancing the overall efficiency and effectiveness of surveillance. Though authority will ultimately reside with a human operator it is to be expected that an increasing amount of decisions will eventually be delegated to software agents.

4.5 Provisional conclusion

Making sense of large amounts of data is a difficult task that traditionally was given to human operators. However, the problem of information overload has prompted public and private parties to employ information and communication technology to aid human operators in their surveillance tasks. To an increasing extent artificial intelligence is used to help find, prepare, and analyse data in order to elicit (previously unknown) information and possibly knowledge. In this chapter we studied some of the ways in which software agents can be used to facilitate and integrate surveillance. Based on current and near future applications of software agents we can establish that they are primarily used for the following three purposes.

Mediation services and query brokering
The current breed of software agents is primarily used to provide logical and semantic interoperability between heterogeneous and disparate data sources. Software agents can help take away the technical barriers that exist in integrating different data sources. Data mining might benefit greatly from agent technology, a supposition that is acknowledged by the intelligence community. Software agents, along with other artificial-intelligence technologies, can help connect the dots and make sense of massive amounts of data.

Augmenting human operators
A second important area in which agent technology is applied is in augmenting human operators. Software agents can help human operators to be more effective in the execution of their tasks for instance by automatically finding,

filtering, and fusing relevant information, removing the need to do mundane tasks, and giving decision support.

Replacing human operators
By continuously monitoring data sources software agents could eventually, at least in part, remove the need for human operators. Examples of monitoring tasks that can be performed by software agents are the operation of CCTV and surveillance of the internet.

The general impression we may obtain from the examples listed above is that the current implementations of agent technology are still fairly limited, but that more extensive use is considered judging from the ambitious research programs that have been proposed, some of which are already conducted. A second impression we may get from the abovementioned examples is that agent technology is almost never used as a stand-alone technology, but is used in conjunction with other artificial-intelligence technologies.

In section 4.4 we have looked at some of the possible future applications of agents. Advances in the field of artificial intelligence will undoubtedly make software agents more intelligent and autonomous. This will allow agents to execute more difficult tasks and will enable them to facilitate and integrate surveillance more effectively. Currently software agents employed for surveillance tasks are relatively simple and do not possess great autonomy both in a legal sense and a technical sense. Given the developments in the field of artificial intelligence however, it is to be expected that more advanced applications will be developed over the coming years. When agents become more autonomous in a technical sense and a legal sense they may significantly alter the surveillance landscape.

In conclusion we may state that while agent technology is not yet used extensively, it is likely that software agents used in conjunction with other artificial-intelligence technologies will have a profound impact on the way in which surveillance is conducted in the (near) future. This will in turn influence privacy and (individual) liberty, which will be topic of the next chapter.

5 The right to privacy

Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society.
Samuel Warren and Louis Brandeis

Surveillance is less effective if people have the ability to hide themselves from the observing gaze. Therefore, many people feel that the negative effects of surveillance can be adequately countered by invoking the right to privacy. Privacy has thus become one of the primary means of protection against surveillance and control.

Privacy is not a static object that can be captured and defined, it is always context related, making it impossible to define it without referring to a complex set of social, cultural, religious, and historical parameters from which it derives its meaning (Gutwirth 1998, p. 40). The goal of this chapter is not to try and come to an incomplete definition of privacy, but rather to provide a better understanding of the meaning and importance of privacy in the context of software agents and control.

In order to gain a better understanding of the right to privacy we must first appreciate why an individual needs privacy and examine the dimensions of human life to which a right to privacy could apply. I shall describe the conceptions of privacy most common in contemporary western thought in section 5.1 and the dimensions of privacy in section 5.2. In section 5.3 I shall focus on the constitutional protection of privacy. The changing face of privacy will be the subject of section 5.4 and informational privacy, which developed as a result of the changing face of privacy, will be the subject of section 5.5. I shall discuss the relationship between electronic surveillance and privacy in section 5.6. In sections 5.7 through 5.12 an overview will be given of the right to privacy in positive law. The chapter shall be concluded with some thoughts about risk justice in section 5.13, and a provisional conclusion in section 5.14.

In sections 5.7 through 5.12 I shall give an overview of the legal frameworks for the Netherlands and the United States. I have chosen the Netherlands and the United States because their approach to dealing with the legal issues surrounding electronic surveillance and privacy differs to a certain extent. The legal system of the Netherlands has its roots in the civil law tradition and is therefore much more focused on statutory law, while the legal system of the United States has its roots in the common law tradition and therefore places

much more emphasis on precedents set by the judiciary. By studying both legal frameworks we can establish whether agent-enabled surveillance impacts the civil law countries, the common law countries, or both. While I shall examine both legal frameworks it is not my goal to compare these legal systems and determine which is better suited to deal with agent-enabled surveillance. Moreover, it is not my goal to single-handedly amend the legal frameworks of both the Netherlands and the United States. Rather I shall give general recommendations that can be implemented in both legal frameworks.

Before we start with examining the right to privacy I would also like to remark the following. We can differentiate between the application of the right to privacy in the relationship between citizens and public administration (most notably in the area of law enforcement) and the application of the right to privacy between private entities (such as businesses and individuals) in their relation to one another. The difference in the application of the right to privacy in various societal relationships is clearly reflected in the law. Though I shall start with giving a general description of privacy, I shall focus on the right to privacy in the public sector, most notably in the area of law enforcement and national security, when I discuss the legal framework for the protection of privacy. While threats to privacy and liberty in the private sector certainly exist, I feel the possible risks of agent-enabled surveillance to privacy and liberty are both greater and more acute in the context of state surveillance. Therefore, this thesis will focus solely on the relation between surveillance and privacy and the accompanying legal framework in the light of surveillance exercised by the state.

5.1 Conceptions of privacy

The need for privacy is probably as old as mankind itself. While convincing evidence of such an assumption is hard to give, anthropological, biological, and sociological studies suggest that even in primitive societies and the animal kingdom, individuals have always had a desire for some sort of privacy (Westin 1984, p. 56-74). Virtually all societies, both primitive and modern, have techniques for setting distances and avoiding contact with others in order to establish physical boundaries to maintain privacy (Wagner DeCew 1997, p. 12). As to why these techniques are invoked and what interests they are meant to protect, is a matter that can only be determined by looking at the relevant social context.

A person who is absolutely alone has no need for privacy. Taking this into consideration we can establish that as a value privacy is only meaningful when more than one person is involved. Privacy, in other words, is always dependent on a social context that differs from group to group, and from culture to culture. The way we view and value privacy is thus for the greater part determined by our cultural, philosophical, and political viewpoints. In our

modern society privacy performs several important functions for individuals, which has led to corresponding conceptions of privacy.[1] I have selected five conceptions of privacy, *viz.* (1) privacy as prerequisite for personal autonomy, (2) emotional release, (3) limited and protected communication, (4) self-evaluation, and (5) privacy to minimise burden. They are the most common in the privacy discourse. They have been mainly derived from Alan Westin's *Privacy and Freedom* (1967, p. 31-39), because I feel Westin's work still gives one of the best summaries of the critical functions privacy fulfils in society.

Personal autonomy

The first conception is that of privacy as a prerequisite for personal autonomy. This fundamental conception of privacy has its basis in individualism. In democratic societies there is a fundamental belief in the uniqueness of the individual, his basic dignity, and his worth as a human being (Westin 1967, p. 33). In order to safeguard personal autonomy and individuality, one must be allowed a private space free from any outside influences. In this 'inner sanctum of the self' the individual can be alone with his deepest thoughts and feelings. If it were not for the psychological barrier raised by privacy against the outside world, the individual would at any time be open to outside scrutiny and judgement. Things like unwanted (internal) searches of the body, intimate behaviour or peculiarities displayed to the outside world, and intrusions of the home, all encroach upon our sense of human dignity (Bloustein 1984, p. 156). Privacy acts as a protective boundary that shields the individual from the inquisitive gaze of third parties. When an individual's core self can be invaded without permission, or even without knowledge, dignity is diminished (Marx 2001, p. 157).

An important aspect of human dignity is the right to individual liberty. As mentioned several times before, knowledge is power. So, the more I know about a person, the greater the degree of control I can exercise over that individual. Privacy places a limit on what the state and other parties can and may know about us by creating an impregnable personal sphere. In this regard privacy acts as a *limit to* the *power* that can be exercised over us by third parties, most importantly the government. Privacy can thus be seen as a countervailing force against power and control.

Emotional release

The second conception of privacy is that the space privacy allows for experiencing emotional release. For almost every individual there is a distinction between his private self and his public selves. I deliberately use the plural 'selves', because the representation of the self in public life usually differs from

1 Apart from individual privacy we can also distinguish organisational privacy, where the right to privacy enables, for instance, companies to conduct their business without having to reveal all their internal processes to the outside world.

one social context to another. In a sense we all continuously act out different roles and display different parts of our personality, depending on audience and situation (Goffman 1959, p. 55-57). For instance, how we behave in the presence of our family or peers might be totally different from the conduct we display in our professional lives. As important as these 'masks' are for social interaction, it is essential for our mental welfare to be able to let them down every now and then and be completely ourselves, including all the ill-mannered aspects of our personality we usually hide from the outside world. Privacy in this sense enables us to experience emotional release (Westin 1967, p. 36), allowing a break so to speak, from the strenuous task of social interaction. A second important aspect of this conception of privacy is that it allows for the creation of social boundaries. Rosen (2000, p. 20) defines privacy as the claim to a social boundary that protects us from being simplified, objectified, and judged out of context. Private information that crosses the social boundary from the private to the public domain (or from one social context to another) without our knowledge or consent can very easily be placed out of context, leading to a judgement of our character that is most likely inaccurate. In his book *the Naked Crowd*, Rosen (2004, p. 161) emphasises the importance of privacy when it comes to judging a person:

> "It is impossible to know someone on the bases of snippets of information, genuine knowledge is something that can be achieved only slowly, over time, behind a shield of privacy, with the handful of people to whom we've chosen to reveal ourselves whole. And even those who know us best may not know us in all of our complicated dimensions."

The problem of selective (mis)interpretation is made all the more acute by technological devices that enable us to record text, sound, and vision. These searchable (digital) records are very susceptible to selective interpretation.

Limited and protected communication

The third conception of privacy to be discussed is that of privacy as a means of limiting and protecting communication. When at all times we would say what we are thinking or feeling, the possibility of any civilized social interaction would be utterly destroyed. While this might sound like a plea for structural dishonesty to one another sanctioned by the right to privacy, it is in fact not. It is an undeniable reality that we are dependent on some form of discretion when we interact with people. We cannot always say what we think about a person, for if we did we would probably hurt or anger a great many people along the way. This also goes for the instances when we talk about others while they are not present. There are times when we talk about people to others, for instance, to vent our anger or frustration, in a way they might not appreciate. Privacy offers us the necessary assurance to be candid about our feelings without having to fear that we might offend someone.

Limited and protected communication also acts as a limit to power since it prohibits third parties, most notably government agencies, from placing our communication under scrutiny. If it were not for the protection of communication it would be impossible to share our thoughts and feelings, for instance, about the government, with others without the fear of being prosecuted for possibly libellous texts.

Self-evaluation
Every individual needs to integrate his experiences into a meaningful pattern and exert his individuality on events (Westin 1967, p. 36). We all need time to think things through and that can be done best when we are alone with our thoughts. Privacy offers the individual the seclusion necessary for self-evaluation and introspection. Only when we are truly alone we can contemplate (1) our behaviour and that of others, (2) events that haven taken place, and (3) thoughts we have had. Without privacy we simply would not have the time to process all the information that is presented to us. A second important aspect of the self-evaluation enabled by privacy is the time necessary to form, structure, and evaluate our opinions and arguments. Arguments, opinions, and creative work all need time to mature and without privacy this would become impossible.

Minimising burden
The last conception of privacy that I wish to address is that of privacy as a means to minimise burden. Our private life is often disturbed by outside influences. Those disturbances can be a nuisance and even a burden, especially if they occur frequently. Therefore, intrusions into our private life should be kept to a minimum. The right to privacy provides us with a means to protect ourselves from these unwanted, burdensome intrusions. When legitimate disturbances do occur the burden they place upon the individual should be kept at a minimum. An example to illustrate this conception of privacy is unsolicited commercial email, or 'spam'. In both the Netherlands and the United States privacy legislation is used to protect individuals from unsolicited commercial email because the unwanted interference caused by spam places an unnecessary burden on the individual.

The relevance of privacy
The right to privacy protects all the conceptions of privacy enumerated above. With regard to the subject matter of this thesis I feel the conception of privacy as personal autonomy (in particular privacy as limit to power) is most relevant when it comes to surveillance. Thus, it is predominantly in the light of this conception that I shall examine the right to privacy when it comes to agent-enabled surveillance.

5.2 Dimensions of privacy

In law, privacy refers to a situation in which the private sphere of the individual is respected (Blok 2002, p. 323). What the 'private sphere' exactly entails is not entirely clear, as is to be expected from such a broad term. A common approach to solving the problem of accurately describing the private sphere is specifying the different dimensions it encompasses. Although such an approach can neither fully capture the essence of privacy, nor provide conceptual unity, it does help in building a framework relevant to the problem definition of this thesis. The following seven dimensions are most common in legal discourse: (1) the body, (2) the mind, (3) the home, (4) intimate behaviour, (5) correspondence, (6) family life, and (7) personal data (Nieuwenhuis 2001, p. 31).

1 The body
In many societies, at least in western society, people want to hide part of their bodies from the prying eyes of others. The right to shield our naked bodies from view is one of the oldest elements of privacy. The integrity of the human body is another element of this dimension of privacy. It refers to the fact that the human body should not be subjected to unwanted scrutiny in the form of searches or the removal of body materials.

2 The mind
In close relation to the integrity of the human body is that of the mind. Analogous to the right to integrity of the human body, it could be argued that there is a right to integrity of the human psyche. The integrity of the human mind is, like many other dimensions of privacy, essential for the human right to self-determination. By guarding our minds from outside scrutiny and influences we ensure that our thoughts can develop freely. Whether thoughts entrusted to paper or to a computer form a part of this dimension remains the subject of debate.

3 The home
Privacy of the home is the right to shield the physical space of one's home from the influence of outsiders. The sanctity of the home is one of the oldest dimensions of privacy. In almost every modern society the home is protected from unlawful intrusion, search, and seizure by the government.

4 Intimate behaviour
We all want to keep some parts of our life to ourselves. The right to keep our physical behaviour (for instance, sex life) hidden from the outside world is one element of this right, the other being our thoughts and with whom we share them.

5 Correspondence
The right to keep our intimate behaviour shielded from the outside world extends itself to the expression of our thoughts in or through communication. What the boundaries of the right to privacy of correspondence are remains unclear. If a complete right to privacy of correspondence is assumed, any investigation into one's correspondence is deemed unlawful. A more limited view is that only investigation of private conversation (thus excluding professional correspondence) is protected.

6 Family life
The right to an undisturbed family life includes the freedom to form a family, to enjoy each other's presence and to live with them according to one's own sense of good.

7 Personal data
In the last decades privacy protection has grown to include the protection of personal data. The importance of personal data as a dimension of the private sphere is the direct result of the rapid proliferation of information and communication technology.

Oftentimes these seven dimensions are categorised into the following three 'spheres of privacy':

Corporeal privacy, which includes the privacy of the (1) body, (2) the mind, and (3) intimate behaviour.
Relational privacy, which includes the privacy of (3) intimate behaviour, (4) the home, (5) the correspondence, and (6) family life.
Informational privacy, made up of (7) personal data, and (5) correspondence.

5.3 The constitutional protection of privacy

The amount of privacy granted to an individual is always balanced against society's need for openness and disclosure. Ideally, individuals should be able to enjoy the maximum amount of privacy, but there are instances where the legitimate interests of society (for instance, public health or security) may outweigh the individual's right to privacy (Etzioni 1999, p. 8).[2] In order to maintain a proper balance between the common good and the individuals right to privacy, laws are enacted that place limits on the interferences that may be made by third parties, while at the same time allowing some room for interferences is necessary in a democratic society.

2 I shall discuss the issue of balancing privacy and security further in chapters 8 through 10.

5.3.1 International privacy legislation

The right to privacy is recognised by most, if not all, democratic states in the world. The universal recognition of the right to privacy is clearly reflected in international law. On a global scale the Universal Declaration of Human Rights and the International Covenant on Civil Rights and Political Rights are most important. I shall briefly describe both in this section.

Universal Declaration of Human Rights (1948)
On December 10 1948, The General Assembly of the United Nations adopted the Universal Declaration of Human Rights (UDHR).[3] Though at its inception the treaty was viewed by most nations as a non-binding agreement without the force of law, the UDHR has effectively acquired force of law through its incorporation in national law and subsequent binding treaties on international law (Rotenberg 2003, p. 316). In Article 12 of the UDHR the right to privacy recognised that:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks."

Article 12 served as the basis for the subsequent codification of the right to privacy in the International Covenant on Civil Rights and Political Rights, the European Convention for the protection of Human Rights, The United Nations Convention on the Rights of the Child, and the American Convention on Human Rights (Rotenberg 2003, p. 316).

International Covenant on Civil Rights and Political Rights (1976)
Though the UDHR is a very important document when it comes to human rights, it is *de jure* non-binding. When the General Assembly adopted the UDHR in 1948 work was started on a legally binding covenant that would enforce the protection of the UDHR. The same commission that drafted the UDHR, the Commission on Human Rights, carried out this work. However, by 1951 disagreement within the Commission was so bad that the General Assembly intervened. The commission which was split along east-west lines could not agree whether the focus of the Covenant should be on political or economic rights since both featured in the UDHR. To end the stalemate, the General Assembly decided to split the UDHR into two separate documents: (1) the Covenant on Civil and Political Rights and (2) the Covenant on Economic, Social, and Cultural Rights. The International Covenant on Civil Rights and Political Rights (ICCPR) was finally adopted by the United Nations in 1976, the United States ratified the ICCPR in 1992.[4]

3 G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948).
4 United Nations Treaty Series No. 14668, vol 999 (1976), p. 171.

Since the ICCPR was based on the UDHR many of its provisions are similar. Article 17 of the ICCPR warrants the protection of the personal sphere and is identical to Article 12 of the UDHR:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks."

The Covenant establishes the Human Rights Committee to monitor its implementation by considering periodic reports from states parties.

5.3.2 The constitutional protection of privacy in the Netherlands

The constitutional protection of privacy in the Netherlands is guaranteed through the Dutch Constitution and the European Convention for the Protection of Human Rights. In this subsection I shall only give a brief description of the constitutional protection of privacy in Dutch legislation and focus primarily on the European legislation. The reason for this is that when it comes to judging possible infringements on the right to privacy, the European Court of Human Rights is the highest institution before which a case can be brought.

The Dutch Constitution
The protection of privacy in the Netherlands is guaranteed by article 10 of the Dutch Constitution (Grondwet). Paragraph 1 of article 10 guarantees the right to privacy:

> "Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament."

Since the paragraph is technology independent, it extends to all dimensions of the right to privacy. Still, the second and third paragraph provide additional protection for the informational privacy:

> "Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.

> "Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament."

A separate article of the Dutch Constitution is devoted to the privacy of correspondence. Article 13 of the Dutch Constitution protects the secrecy of

letters as well as the secrecy of communications conducted by means of telephone and telegraph:

> "The privacy of correspondence shall not be violated except in the cases laid down by Act of Parliament, by order of the courts.
>
> "The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament."

What is relevant to note with regard to the subject matter of this thesis is that article 13 is technology dependent.

The European context

While most European nations have a long history when it comes to constitutional rights, it wasn't until after the Second World War that a human rights treaty for Europe was drafted. Shortly after the adoption of the Universal Declaration of Human Rights, the Council of Europe adopted the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).[5] The European Convention for the protection of Human Rights defines the constitutional protection of privacy in Europe in article 8.[6] The first paragraph of Article 8 ECHR deals with the protection of private and family life and reads as follows:

> "Everyone has the right to respect for his private and family life, his home and his correspondence."

Since the right to privacy is not absolute, the second paragraph of article 8 ECHR determines under what circumstances public authorities are allowed to encroach upon the right to privacy:

> "There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

---

5 *Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms*, Rome 4.XI.1950.

6 Apart from the European Convention on Human Rights, there is also the Charter of Fundamental Rights of the European Union that was 'solemnly proclaimed' by the European Parliament, the Council of the European Union, and the European Commission in December 2000. However, since the Charter of Fundamental Rights is not a legally binding document (it is not a treaty) it is of less importance to the subject matter of this thesis. Moreover, since the text of the Charter is generally in line with the ECHR, I shall not discuss it any further.

When a public authority has illegitimately violated an individual's right to privacy, the individual has the right to seek effective remedy through the European Court of Human Rights pursuant article 13 of the ECHR.

The Court will first establish whether an interference into the individual's private sphere has actually taken place. When an interference has taken place, article 8 ECHR is applicable. Next, the Court determines whether the interference is justified. For an interference to be justified it must be in accordance with paragraph 2 of article 8 ECHR. The second paragraph sets forth three important requirements.

First, any interference must be 'in accordance with the law', meaning there has to be a clear legal basis for the interference, the law establishing this basis should be readily accessible, and it should meet the standards of foreseeability. In other words, the law must be of such a quality that it is sufficiently clear in its terms to give an adequate indication of the circumstances in which and the conditions on which public authorities are empowered to resort to a given investigative power. Furthermore, the law must define the scope and manner of exercise of such a power clearly enough to ensure adequate protection from arbitrary interference.

Second, any interference by a public authority into the personal sphere must pursue a legitimate aim. This means that the interference must pursue the interests of national security, public safety or the economic well being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

Third, the interference must be 'necessary in a democratic society', in other words the interference must be proportionate.

In several landmark cases the European Court of Human Rights interpreted the requirements of paragraph 2 of article 8 ECHR. Of particular interest to the subject matter of this thesis are the Court's views on the 'quality of the law' and the 'reasonable expectation of privacy' which flow forth from the requirement that any interference must be in accordance with the law.

Quality of the law

On the subject of surveillance and surveillance technologies the Court has delivered several important judgements. These judgements place special emphasis on the quality of the law. In the case of *Krüslin v. France* the Court held that a French wiretapping law lacked the requisite foreseeability, as it defined neither the categories of people liable to have their phones tapped nor the types of offences that justified a wiretap.[7] The complainant, Krüslin, had been arrested on the suspicion that he was involved in a murder case. The suspicion arose when information, gathered from a wiretap that was installed in the house of a friend (Mr. Terrieux, also a suspect) where Krüslin

7 Case of Krüslin v. France, case nr. 7/1989/167/223.

was staying, implicated Krüslin in the murder. Though it was Terrieux's line they were tapping, the police also intercepted and recorded several of Krüslin's conversations, and one of these led to proceedings being taken against him. The telephone tapping therefore amounted to an 'interference by a public authority' into Krüslin's private life. Krüslin claimed the use of the wiretap constituted a breach of article 8 ECHR as there was no basis for a wiretap in French law. Though the Court rejected this argument it did find that the quality of the law was lacking in the area of foreseeability. With regard to the law that governs the application of special investigative powers such as wiretaps the Court stated:

> "Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."

The Court concluded that French law, written and unwritten,

> "(...) did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities."

As such Krüslin did not enjoy the minimum degree of protection to which citizens are entitled under the rule of law in a democratic society.

In the case of *Kopp v. Switzerland* the legitimacy of a wiretap was also contested. In this case the federal prosecutor of Switzerland ordered the phone line of a Swiss law firm to be tapped. The complainant argued that the wiretap constituted a violation of article 8 ECHR. The Court held that a violation of privacy by a public authority had indeed taken place and that this violation was not in accordance with the law. While there was a basis in Swiss law (the Federal Criminal Procedure Act) that was readily accessible, the quality of the law failed to meet the standards of foreseeability. As the wiretap constituted a serious interference with private life and correspondence, it had to be based on a law that was particularly precise, which the Federal Criminal Procedure Act was not. Analogously the Krüslin case, an important factor in this decision was the fact that the technology available for wiretapping and surreptitious surveillance was continually becoming more sophisticated.

It is clear from these and other cases before the Court that the quality of the law, more in particular its foreseeability, is an important requirement when it comes to technologically advanced surveillance practices.[8] Therefore, when

8 Other cases include *Hüvig v. France* (case no. 4/1989/164/220) and *Amann v. Switzerland* (application no. 27798/95, Judgement Strassbourg).

it comes to software agent-enabled surveillance it is imperative that a law that is particularly precise governs its application.

The reasonable expectation of privacy
In the case of *Lüdi v. Switzerland* we see that the reasonable expectation of privacy criterion, which developed in the United States Supreme Court's jurisprudence, has also found its way into the jurisprudence of the European Court of Human Rights.[9] Lüdi, a Swiss national was arrested on suspicion of drug trafficking. He was exposed when an undercover agent bought drugs from him.[10] Lüdi claimed that this was a violation of his private life and that this constituted a violation of article 8 ECHR. The Court however held that the use of an undercover agent, either alone or with the telephone interception, did not affect Lüdi's private life since he must have been aware of the fact that he was engaging in a criminal activity and that this activity entailed the risk that he would be approached by an undercover agent whose task it would be to expose him.

5.3.3 The constitutional protection of privacy in the United States

When it comes to the constitutional protection of the right to privacy in the Unites States the most striking feature is that it is not explicitly mentioned in the Constitution. Instead, the constitutional protection of the right to privacy in the United States has developed through the jurisprudence of the federal courts. The United States Supreme Court has repeatedly interpreted many of the amendments constituting the Bill of Rights to provide protection to a variety of elements of individual privacy. The Court has found protections for privacy in the First Amendment provisions for freedom of expression and association, the Third Amendment restriction on quartering soldiers in private homes, the Fourth Amendment prohibition on unreasonable searches and seizures, the due process clause and guarantee against self incrimination in the Fifth Amendment, the Ninth and Tenth Amendment reservations power in the people and the States, and the equal protection and due process clauses of the Fourteenth Amendment (Minow *et al.* 2004, p. 21-22).

The Fourth Amendment to the Constitution
The constitutional protection of the right to privacy in the United States has primarily been derived from the Fourth Amendment to the United States Constitution, which provides protection from unreasonable searches and seizure. The text of the Fourth Amendment reflects the resentment of the

9 I shall discuss the reasonable expectation of privacy criterion more at length in subsection 5.3.3.
10 In an earlier stage his telephone had also been tapped.

colonists against the practice of the British Crown to issue general warrants that made general searches possible.

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but on upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The scope and meaning of the Fourth Amendment has been clarified in a number of Supreme Court cases. An early case regarding the scope of the Fourth Amendment and its relation to privacy is *Boyd v. the United States*.[11] In this case the Supreme Court held that the Fourth Amendment is applicable to "all invasions (…) of the sanctity of a man's home and the privacies of life." A subpoena issued to Boyd to produce a set of invoices was deemed unconstitutional on the grounds that it encroached upon "his indefeasible right of personal security, personal liberty, and private property." In *Boyd v. the United States* a common law conception of privacy (i.e., a right to privacy closely linked to property) was put forth for the first time.

The common law interpretation of the right to privacy would remain dominant well into the twentieth century. But gradually the limitations of a right to privacy linked closely to property became apparent, in part due to technological advances. In *Olmstead v. the United States* we see the right to privacy is still closely linked to property.[12] The Supreme Court held that tapping a phone line outside someone's house is not a violation of the Fourth Amendment since no search or seizure is conducted. *Olmstead v. the United States* relied upon the Supreme Court's physical intrusion conception of privacy (Solove 2004b, p. 197), a view that would come to be known as the 'trespass doctrine'. In the case of *Goldman v. the United States* the trespass doctrine was held.[13] In this case the recording of a conversation through the walls of a house by means of a detectaphone did not constitute a violation of the Fourth Amendment since there was no trespass on to the property of the petitioner.

In 1967, *Olmstead v. the United States* and *Goldman v. the United States* were reversed by *Katz v. the United States*.[14] In this decision the Supreme Court held that the legitimacy of interference into the personal sphere is determined by an individual's 'reasonable expectation of privacy'. This is a twofold requirement as Justice Harlan explains in his concurring opinion:

> "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective)

11 Boyd v. the United States, 116 U.S. 616, 630 (1886).
12 Olmstead v. the United States, 277 U.S. 438, 478 (1928).
13 Goldman v. United States, 316 U.S. 129 (1942).
14 Katz v. the United States, 389 U.S. 347, 351 (1967).

> expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'. Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."

The case was as follows: Katz was charged with illegally transmitting wagering information by telephone across state lines. Katz' transgressions came to light when FBI agents overheard his conversations through a wiretap they had attached to the public telephone booth where Katz made his regular phone calls. The Court of Appeals found that there was no violation of the Fourth Amendment since there was no physical entrance into the area occupied by Katz. However, the Supreme Court held that:

> "The Government's eavesdropping activities violated the privacy upon which petitioner justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."

Moreover, the Supreme Court held that:

> "Because the Fourth Amendment protects people rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure. The 'trespass' doctrine of Olmstead v. United States, 277 U.S. 438, and Goldman v. United States, 316 U.S. 129 , is no longer controlling."

Since *Katz v. the United States* the conception of the right to privacy linked so closely to (physical) property has been abandoned in favour of a right that protects the individual itself. The reasonable expectation of privacy has become the dominant doctrine, though, in the years following *Katz v. the United States*.[15] Within the light of new technologies the 'reasonable expectation of privacy' test has thus become the touchstone for how the Fourth Amendment applies (Kerr 2004).

5.4 THE CHANGING FACE OF PRIVACY

Privacy as both a value and a right is the product of a complex set of historical, social, legal, and cultural factors. Accordingly, the way we think about privacy changes over time, a process in which technology plays an important part.

---

15 Even though the reasonable expectation criterion has shifted somewhat towards a 'legitimate expectation of privacy' as a result of more conservative justices within the Supreme Court (Blok 2002, p. 162).

Without any doubt the most important change in the way we view privacy that has taken place over the last few decades has been the inclusion of personal data into the private sphere.

Many of the activities in our society have become, or are becoming, in large parts dependent on the processing of (personal) data. The main drive behind this development is society's demand for speed, convenience, mobility, efficiency, and risk management in social and economic relationships. The rapid proliferation of personal data is mainly a result of advances in information and communication technology. The advent of information and communication technology has led to a sharp increase in the amount of data that is being collected on individuals at various occasions, much of which is permanently stored for future reference.

With emergence of electronic recordkeeping two distinct lines of privacy theory developed (Taipale 2003, p. 55). The first line is based on the traditional notions of the 'private sphere' and is concerned with surveillance and (physical) intrusion. The second line is based on control of personal information about the self and is more concerned with self-determination and autonomy (Cohen 2003). Taipale (2003, p. 56) has made a further distinction between the different interests in informational privacy, *viz.* anonymity, secrecy, and autonomy. Anonymity is the interest in not being associated with one's private affairs or activities, secrecy is the interest in not having those private affairs revealed or made public, and autonomy is the interest in being free in action. While anonymity, secrecy, and autonomy are all important when it comes to the issue of surveillance and control, I shall explore the issue of autonomy somewhat further. The reason for this is that it is most closely related to the issue of surveillance and control and has impacted the thinking about privacy a great deal in recent times.

The digital traces that we leave behind in the course of our (daily) interactions, can be monitored, recorded, searched, and compiled into a fairly accurate 'digital copy' of our personality. As technology advances, these digital copies become increasingly accurate and easy to access and interpret. The profiling of our 'digital self' raises important questions with regard to the persons and organisations that create or obtain these profiles and the goals to which they are used. As mentioned before, knowledge is power. While Bacon applied this adage to our physical environment, it is equally applicable to human beings. As our digital copies become increasingly accurate, the effectiveness of the modes of control employed also increases. By placing a limit on the amount of information that is available on us, we lessen the ability of third parties to predict, regulate, or control our behaviour effectively. One way of reducing the amount of data that can be collected on us, is shielding ourselves (and our personal data) from the inquisitive gaze of others. If we regard privacy as the right to be let alone, it seems an ideal candidate for limiting the amount of information that is known about us.

As a result of technological advances that made the problem mentioned in the previous paragraph progressively more acute, the focus of the privacy debate has in the past decades shifted from the protection of the 'classic' dimensions of privacy (the body, the home, and the correspondence), to the protection of personal data (Blok 2002). As people grew more aware of the potential misuse of personal data for control, the conception of privacy as a limit to power became more prominent. Public fear of a 'database nation' struck as early as the 1960s when computers started to automate personal data processing and storage. To address the growing threat of excessive control through personal information, the scope of the right to privacy was broadened to allow for the incorporation of personal data into the private sphere. Alan Westin (1967) in his seminal work *Privacy and Freedom*, was among the first to connect the issue of personal data protection to the conception of privacy as a limit to power. Privacy is described by Westin (1967, p. 7) as: "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated." The definition of privacy as proposed by Westin has led to the notion of 'informational privacy' and the idea of 'informational self-determination'. This fundamentally changed the right to privacy from its 'classic' form (i.e., the right to the protection of a personal sphere) to its current incarnation as a means to limit the abuse of personal data.

5.5 INFORMATIONAL PRIVACY

As we have seen the rise of information and communication technology played a significant role in the development of the right to privacy. The automated processing of personal data using computers and accompanying database technology changed the face of privacy considerably. The new face of privacy also prompted changes to the codification of the right to privacy.[16] This process started in the early seventies of the twentieth century with the drafting of the *Fair Information Practice Principles*.

5.5.1 Fair Information Practice Principles (1973)

In 1973 the United States Department of Health, Education, and Welfare drafted a seminal report titled *Records, Computers and Rights of Citizens* that contained a *Code of Fair Information Practices*. These Fair Information Practices

16 It is important to note that scope of data protection law is broader than that of the right to privacy (Hustinx 2004, p. 270). As such, data protection law does not depend on a distinction between the public and the private for its application. However, data protection law is still intimately linked to the right to privacy and the individual.

consist of five basic principles to which every data processing party should adhere.

- There must be no personal data record-keeping system of which the very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent the misuse of data.

5.5.2 OECD Privacy Guidelines (1980)

An important (international) development in the regulation of informational privacy was the adoption of the *Recommendation Concerning and Guidelines Governing the Protection of Privacy and the Transborder Flow of Personal Data* by the Organisation for Economic Cooperation and Development (OECD). Without the processing of personal data much of our social and economic activities would be far less efficient and effective, or would become impossible altogether. As such, there must be room for a free flow of personal data. The OECD Privacy Guidelines were drafted to create a framework that would allow for the transborder flow of personal data while safeguarding the privacy of the individual. They set forth a path to privacy based on the following eight principles (Rotenberg 2003, p. 328).

Collection Limitation Principle
This principle states that personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. Furthermore there should be limits to the collection of personal data.

Data Quality Principle
This principle states that any personal data collected should be relevant to the purposes for which they are to be used and when used should be accurate, complete, and kept up-to-date.

Purpose Specification Principle
This principle states that the purpose of the collection of any personal data should be specified not later than at the time of data collection and the sub-

sequent use limited to the fulfilment of those purposes, or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle
This principle states that personal data should not be disclosed, made available, or otherwise used for purposes other than those covered by the purpose specification.

Security Safeguards Principle
This principle states that any personal data collected and used should be protected by reasonable security measures to minimise the risk of unauthorised access, destruction, use, modification, or disclosure of personal data.

Openness Principle
This principle states that there should be a general policy of openness about developments, practices, and policies with respect to personal data. It further states that means should be readily available of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and residence of the data controller.

Individual Participation Principle
This principle acknowledges certain rights of data subjects with regard to their personal data. The first right a data subject has is the right to obtain confirmation from a data controller whether his information is being processed. Furthermore, the data subject has the right to have this information communicated to him within a reasonable time, in a reasonable manner, and in a form that is readily intelligible to him. If such information cannot be communicated, the data subject must be given reasons as to why it cannot be communicated, as well as the right to challenge this decision. Finally the data subject has the right to challenge data relating to him, and if successful have it erased, rectified, completed, or amended.

Accountability Principle
The final principle holds data controllers accountable for complying with measures that give effect to the above stated principles.

The principles laid down in the OECD Guidelines are still used. The OECD Privacy Guidelines have played an important part in the creation of the European personal data protection regime, for which the groundwork was laid in 1981.

5.5.3 Council of Europe Convention on Privacy (1981)

Inspired by the OECD Privacy Guidelines the Council of Europe concluded the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* in 1981. The Convention entered into force in 1985. As the Council of Europe worked closely with the OECD the Convention closely resembles the OECD Privacy Guidelines. For this reason I shall not enumerate the individual provisions of the Convention as they are roughly the same as the OECD Privacy Guidelines.

5.6 Electronic surveillance and the law

Now that we have discussed the general constitutional protection of privacy and the increased importance of informational privacy, I shall turn to a discussion of the specific legislation dealing with surveillance and privacy in the Netherlands and the United States. I shall devote special attention to those provisions that govern the use of electronic surveillance. I will not give a complete overview of the laws that govern surveillance and privacy, but rather discuss those aspects of the existing legislative framework that are of special interest when it comes to agent-enabled surveillance. During the discussion I shall also take recent legislative developments into consideration.

One of the areas where privacy and individual liberty are particularly at stake, is government intervention for the sake of a criminal investigation, enforcing special laws through monitoring, and maintaining public order (Koops and Vedder 2001, p. 87). It is important to distinguish the use of surveillance methods for a criminal investigation from the use of surveillance for monitoring purposes. While in both cases investigative powers and coercive measures may be employed, the goals at which the use of these powers and measures are aimed differs. Monitoring is aimed at ensuring compliance with specific regulation while a criminal investigation is aimed at determining who committed a crime (Koops and Vedder 2001, p. 24). Therefore, the regulation of the use of investigative powers and coercive measures also differs. The rules governing the use of investigative powers and coercive measures for the purpose of ensuring compliance with specific regulation (such as tax law or environmental law) are usually codified within the special legislation itself. The rules governing the use of investigative powers and coercive measures for the purpose of a criminal investigation are governed by the rules of criminal procedure.

While the investigative methods used for monitoring purposes and those used for a criminal investigation are often alike, there are some investigative methods that may only be used over the course of a criminal investigation. These investigative powers tend to have greater impact on privacy and indi-

vidual liberty, as they are more far reaching.[17] I shall focus on the use of investigative powers for (pro-active) criminal investigations because they are most interesting when it comes to agent-enabled surveillance. Moreover, it is outside the scope of this thesis to discuss the individual investigative powers for every special law.

5.7 Criminal procedure and privacy in the Netherlands

In this section I shall describe the legislative framework for the protection of privacy in the Netherlands. While the European Union has greatly influenced data protection law in the Netherlands, criminal procedure is still a predominantly national affair. Therefore, I shall only discuss the legal framework of the Netherlands, and not focus on the European context.[18] It must be noted however, that international cooperation is becoming increasingly important in Europe, especially in the area of anti-terrorism.

5.7.1 The Data Protection Act

Before we turn to a discussion of the law of criminal procedure and privacy in the Netherlands, a brief discussion of the *Data Protection Act* (Wet bescherming persoonsgegevens) is in order as it is the main piece of legislation that governs informational privacy in the Netherlands.[19] The Data Protection Act, which is based on EU Directive 95/46/EC, provides the general framework for the protection of personal data in the Netherlands. The Data Protection Act is based around the previously mentioned OECD privacy guidelines. The rules it sets forth apply to both public and private data controllers. For the subject matter of this thesis it is of importance that the work of law enforcement agencies and the intelligence community is exempted from the Data Protection Act (see article 2 Data Protection Act).

5.7.2 The Dutch Code of Criminal Procedure

The use of investigative methods is not exhaustively codified in the Dutch law that governs criminal procedure. To some extent, public officials and law enforcement officers may use their own creativity in an investigation. However,

17 I shall not describe the rules that govern coercive measures as they are of little interest to the subject matter of this thesis.

18 I will use the English translation of Dutch terms where possible. Dutch terms will be supplied in brackets when necessary.

19 Wet bescherming persoonsgegevens, *Staatsblad* 2000, 302

those investigative methods that could infringe on the constitutional rights of an individual, need to have a basis in law, more specifically in the rules of the criminal procedure. The investigative powers that can be exercised by public officials for the purpose of a criminal investigation are for the most part defined in the Dutch *Code of Criminal Procedure* (Wetboek van Strafvordering). The Code of Criminal Procedure (CCP) was enacted in 1926 and has since then been updated and amended several times. The CCP is divided into five books of which the first book (articles 1-138c CCP) is most relevant when it comes to the subject matter of this thesis. The first book is most relevant because it regulates amongst other things, the interception of communication, and other provisions on special investigative powers. Those investigative methods that might infringe on the constitutional rights of individuals (for instance, searches and seizures) and the conditions for their use are codified in the CCP and accompanying laws, such as the *Police Act 1993* (Politiewet) and the *General Entry Act* (Algemene Wet op het Binnentreden).

5.7.3 Computer Crime Bill II

With regard to the subject matter of this thesis the *Computer Crime Bill II* (Wetsvoorstel Computercriminaliteit II) is another important piece of Dutch legislation.[20] The Computer Crime Bill II was first introduced to parliament in 1999 and was finally adopted in May 2006. The Computer Crime Bill II is in line with the Cybercrime Convention.[21] Apart from new substantive law on computer-related crimes, several (special) investigative powers and coercive measures were updated, while new coercive measures and special investigative powers were also introduced. I shall discuss these powers in subsection 5.7.4 along with the other special investigative powers.

5.7.4 Special investigative powers

When public officials use investigative powers in the course of a criminal investigation it is highly likely that their application will interfere with the private life of those at whom the investigation is aimed. Therefore, the application of investigative powers must be in accordance with the law. During criminal investigations conducted in the early nineties Dutch law enforcement officers used a range of investigative methods, such as wiretapping and running informants that had no clear basis in the Dutch criminal procedure. As a result neither the courts nor the prosecution could adequately perform their role of supervisor of the police. Quite often this led to the use of policing

20 Parliamentary Series (*Kamerstukken II*), 26 671.
21 Council of Europe Convention on Cybercrime, ETS no. 185, Budapest 23.XI.2001.

methods that were in conflict with the rule of law in a democratic society. This situation ultimately led to a parliamentary inquiry into the criminal investigation methods employed by the Dutch police. The committee of inquiry (named after its chairman Maarten van Traa) investigated the various investigative methods and concluded that they needed a clear basis in the Dutch law. As a result *the Special Powers of Investigation Act* (Wet Bijzondere Opsporingsbevoegdheden) came into effect on the 1st of February 2000. The Special Powers of Investigation Act amends the CCP and governs the application of the special investigative powers. They include amongst others: surveillance, infiltration, pseudo purchase and service, 'looking in' operations, undercover surveillance, the recording of confidential information, and the investigation of telecommunication. I shall discuss those special investigative powers that can be linked to agent-enabled surveillance.

Title IVA of the CCP (articles 126g-126nf) regulates the use of special investigative powers for a 'standard' criminal investigation, while title V of the CCP (articles 126o-126uf) regulates the use of special investigative powers in the fight against organised crime. Because organised crime involves the continuous planning and perpetration of crimes, it was deemed necessary by the legislature that the use of special investigative powers could also be extended to the planning phase of organised crime. As such title V of the CCP regulates the use of special investigative powers in the pro-active phase of a criminal investigation (i.e., before a crime has actually been committed).

Surveillance (article 126g CCP, 126o CCP)

Article 126g of the CCP regulates the use of surveillance (stelselmatige observatie) as an investigative method, article 126o CCP regulates the use of surveillance in the fight against organised crime. Article 126g CCP defines surveillance as: "systematically following a person or systematically observing their whereabouts." Surveillance is deemed systematic when it enables an almost complete picture to be gained of certain aspects of a person's life. This differentiates surveillance in the sense of article 126g CCP from ordinary surveillance or incidental observation. Different factors determine whether surveillance is systematic: the duration of the observation, the place, the intensity, the frequency of the observation, and whether a technical device is used that can do more than enhance the senses.

Systematically following or observing a person is only permitted in the case of a suspected crime and at the order of the public prosecutor. The duration of the surveillance is bound to a maximum of three months, a period that can be extended by three months by order of the public prosecutor. Whether behaviour is observed offline or online does not matter, both the article and the explanatory memorandum do not exclude observation of persons on the internet, therefore surveillance can also be conducted in places such as chatrooms and massive multiplayer online role playing games.

Infiltration (article 126h CCP, 126p CCP)
Article 126h of the CCP regulates the investigative method of infiltration; article 126p CCP regulates the use of surveillance in the fight against organised crime. Covert investigation or infiltration can be defined as: "participating or co-operating with a group of people that is believed to be planning crimes or to have committed crimes."

In any covert investigation there is a serious risk that the covert investigator will have to commit criminal offences, lest his cover be blown. While a covert investigator may commit criminal offences in order to stay undercover, any actions that could give rise to a criminal offence should be listed in the warrant issued by the public prosecutor. While a covert investigator may commit criminal offences he may not incite a person to commit offences other than already planned by the individual. This is known as the 'Tallon Criterion', which was first established in the Tallon case.[22]

Infiltration is only allowed when there is a reasonable suspicion of one of the criminal offences mentioned in article 67 CCP, that given its nature, or its relation to other offences committed by the suspect forms a serious breach of law and order. When it comes to procedural requirements, the most important requirement is that the public prosecutor must give his explicit authority through a warrant.

Pseudo purchase/services (article 126i CCP; 126q CCP)
Article 126i CCP regulates the use of pseudo-purchase or pseudo-services as an investigative method, article 126q CCP regulates the use of pseudo-purchase/services in the fight against organised crime. Pseudo-purchase/service can be described as: "the purchase of goods from, or the supply of services to the suspect." Since a criminal offence could result from the use of this investigative method the Tallon criterion is also applicable to pseudo-purchase/services. In the Special Powers of Investigation Act pseudo-purchase/service was limited to the physical world. The Computer Crime Bill II amended articles 126i CCP and 126q CCP to include online pseudo-purchase/services.

Systematically gathering intelligence undercover (article 126j CCP; 126qa CCP)
Article 126j CCP regulates the investigative method of systematically gathering intelligence undercover. Article 126qa CCP regulates the investigative method of systematically gathering intelligence undercover in the fight against organised crime. We may speak of systematically gathering intelligence undercover when a police officer takes active steps to become involved in the life of a suspect without it being apparent that he is actually a law enforcement officer. A police officer could, for instance, gain intelligence on a suspect through undercover activities, such as visiting places, which the suspect frequents. Systematically gathering intelligence under cover differs from

22 HR 4 december 1979, NJ 1980, 356.

infiltration because the investigating officer is not committing any punishable acts himself. This also means that the undercover work poses fewer risks to the integrity and security of the investigation. Therefore, this investigative method is bound by less stringent requirements than infiltration and pseudo-purchase/service.

Systematically gathering intelligence undercover is only allowed when there is a reasonable suspicion of one of the criminal offence mentioned in article 67 CCP, that given its nature, or its relation to other offences committed by the suspect forms a serious breach of law and order. When it comes to procedural requirements, the most important requirement is that the public prosecutor has got to give his explicit authority through a warrant.

Recording confidential information (article 126l CCP)
Article 126l CCP regulates the recording of confidential information as an investigative method. The article is only concerned with the recording of *confidential* information using a *technical* aid. Communication is confidential when the parties involved have the subjective expectation that their communications are private. The fact that a technical aid must be employed excludes communications that can be picked up without technical aids, such as an audible conversation. Confidential communications can be recorded for investigative purposes using technical equipment such as 'bugs' and scanning devices. To record confidential information, these technical aids must be placed in the suspects' environment. Recording confidential communication in a private residence is subject to strict terms: it is only allowed when it is urgently required for the investigation, the offence under investigation is mentioned in article 67 CCP, and the examining magistrate has given explicit authority.

Investigating telecommunications (Title IVA, section 7, 126m CCP)
Article 126m CCP regulates the use of wiretaps for law enforcement purposes. When an offence poses a serious breach to law and order, an investigation into telecommunications can be ordered. Such an investigation may only be ordered when it is urgently required, the offence under investigation is mentioned in article 67 CCP, and the examining magistrate has given explicit authority. It is the public prosecutor who, after receiving authority from the examining magistrate, issues the warrant to tap a telephone. The public prosecutor is also responsible for the gathering and storage of the acquired data.

An investigation into telecommunications differs from the recording of confidential information in that it is not necessary to enter any physical space occupied by the suspect since a wiretap can be installed at a telecommunications provider.

5.7.5 Wet vorderen gegevens telecommunicatie (Title IVA, section 7 CCP)[23]

In July of 2004 the *Wet vorderen gegevens telecommunicatie* was passed. The bill amends the CCP and provides a statutory basis for demanding telecommunications data for use in a criminal investigation. Increasingly telecommunications data is used in criminal investigations, therefore the use of this investigative power needed a clearer basis in the law of criminal procedure. Articles 126n, 126na, 126nb, 126u and 126ua CCP set forth the rules for the collection of telecommunications data in a criminal investigation. In the context of telecommunications data we can distinguish between traffic data and user data, both of which can be relevant to an investigation.

Traffic data is defined in Article 2a of EU directive 2002/58/EC on Privacy and Electronic Communications as: "data processed for the purpose of conveyance of a communication on an electronic communications network or for the billing thereof." This includes amongst others: data necessary to follow and identify the source of a communication, data necessary to identify the destination of a communication and data necessary to identify the time of a communication.[24] Article 1 paragraph d of the Cybercrime Convention gives a similar definition:

> "traffic data means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."

It is the telecommunications provider that keeps traffic data, and the investigative power is thus aimed at claiming these data from the telecommunications provider. The collection of traffic data is governed by articles 126n and 126u CCP. The collection of traffic data can be ordered by the public prosecutor and is only allowed when the offence under investigation is mentioned in article 67 CCP.

Though traffic data gives information regarding the origin and destination of the communication, it does not identify the person who used or subscribed to the telecommunications service. Therefore, information identifying the subscriber or user of a telecommunications service can also be demanded from the telecommunications service provider. Information that identifies the subscriber or user of the telecommunications service is called user data. Article 126n paragraph b CCP describes a user of a telecommunication service as: "any legal entity or natural person subscribed to a telecommunications service, as well as any legal entity or natural person actually using a publicly available electronic communications service." Any law enforcement officer may request

23 *Staatsblad* 2004, 105.
24 OJ L 201, 31 July 2002.

user data from a telecommunications service provider when there is a suspicion of a crime (see article 126na paragraph CCP), a requirement less stringent than that of the other special investigative powers in the area of telecommunication data.

5.7.6 Wet bevoegdheden vorderen gegevens (Title IVA, section 8 CCP)[25]

A result of liberal surveillance is that people leave information trails over the course of their daily activities in countless private-sector databases. This information can be of interest to law enforcement and intelligence agencies. To ensure law enforcement agencies can gain access to information residing in private-sector databases, the Dutch legislature passed the *Wet Bevoegdheden vorderen gegevens* in 2005. The bill, which amends the CCP, was one of the legislative responses to the terrorist attacks that took place in the United States, Spain, and the Netherlands.

The new coercive measure is codified in section 8 of Title IVA of the CCP and allows law enforcement officers to demand (personal) data stored in databases from *any* third party if it is suspected that the information is of value to a criminal investigation. A writ issued by the examining magistrate is required before any data can be demanded. The demand for data must be sufficiently specified, and therefore the writ must contain an appreciable description of the crime under investigation, and if possible a description of the suspect.

5.7.7 Police Files Act (PFA)

The previous sections of this chapter have dealt primarily with the rules governing the gathering of data by law enforcement agencies. Also of importance is how this data may be processed further and shared once gathered by law enforcement agencies.[26] The *Police Files Act* provides a regulatory framework for the processing of (personal) data by the police. The regulatory structure of the new *Police Files Act* closely resembles that of the OECD privacy guidelines, bringing it into line with the structure of the Dutch *Data Protection Act*. A new legislative framework for the processing of personal data was deemed necessary because advances in information and communication technology made the structure of the old legal framework obsolete. The new

25 *Staatsblad* 2005, 390.

26 Tweede Kamer, vergaderjaar 2005-2006, 30 327, A. At the time of writing the use of (personal) data for law enforcement purposes is still governed by the *Police Registries Act* (Wet Politieregisters). However, since the new *Police Files Act* (Wet Politiegegevens) is set to replace the old Police Files Act soon, I shall only discuss the new legislation.

Police Files Act offers greater room for the processing of personal data by the police, for instance through, data mining.

The Police Files Act describes six different contexts in which police data (including personal data) can be processed, *viz.* the processing of police data for (1) the daily execution of the police task (article 8 PFA), (2) targeted use in order to maintain law and order (article 9 PFA), (3) combating certain forms of crime or behaviour that pose serious threats to law and order (article 10 PFA), (4) automated comparison of police databases (article 11 PFA), (5) managing informants (article 12 PFA), and (6) supporting tasks (article 13 PFA).

The daily execution of the police task (article 8 PFA)
Police data may be processed for the purpose of executing the daily police task. What exactly constitutes the daily police task is clarified in articles 2 and 6 of the Police Act of 1993. Generally speaking, the execution of the daily police task is concerned with 'keeping eyes and ears open'.

Targeted use with the goal of maintaining law and order (article 9 PFA)
When considerable efforts are made for the targeted processing of personal data with the goal of maintaining law and order in a specific case, article 9 PFA applies. The Explanatory Memorandum describes 'targeted processing' as the processing of substantial amounts of structured data relating to certain individuals.[27] This is, for instance, the case when a criminal investigation or an exploratory investigation has started, or in those cases where special investigative powers are used.

As mentioned, article 9 PFA deals with those instances where there is already some knowledge that a criminal act or acts have taken place, or are taking place. As such, the processing of personal data in the context of article 9 PFA is a reactive form of investigation.

Combating certain forms of crime or behaviour (article 10 PFA)
Article 10 PFA is concerned with the targeted processing of personal data in order to gain insight into the involvement of persons in the acts of planning or committing crimes that pose a serious threat to law and order. In article 9 PFA the processing of personal data is centred around a specific case or situation, while article 10 PFA focuses on maintaining a certain information position. While article 9 PFA deals with reactive investigation, article 10 PFA provides a basis for pro-active investigation.

Automated comparison (article 11 PFA)
Article 11 opens up the way for the automated comparison of different police databases. This means that for the purpose of an investigation *ex.* article 9 PFA

27 Tweede Kamer, vergaderjaar 2005–2006, 30 327, no. 3, p. 43.

or 10 PFA, police databases may be compared or matched. This means that police data gathered and processed in the context of an investigation ex. Article 8, 9, or 10 PFA, may also be used in another investigation when the data mining exercise yields a connection.

Managing informants (article 12 PFA)
Police data may also be used for the purpose of managing informants that are being run by the police. Since this context is out of the scope of this thesis I shall not discuss it further.

Supporting tasks (article 13 PFA)
The police may use data gathered in the light of one of the previous contexts for the support of certain police tasks. Since this context is out of the scope of this thesis I shall not discuss it further.

5.7.8 Special investigative powers for the investigation of terrorist activities

In response to the terrorist attacks in Madrid on March 11, 2004, the Dutch government introduced a proposal for a new anti-terrorism bill.[28] Though the murder of Dutch filmmaker Theo van Gogh advanced the sense of urgency and sped up the legislative process, the bill has not yet been introduced. The bill is aimed at making both investigations into terrorist activities and the prosecution of terrorist offences easier. The bill will introduce new offences, far reaching investigative powers, and procedural efficiencies. In the area of (electronic) surveillance the goal is to add two new titles (VB and VC) to the CCP that provide additional investigative powers. With regard to privacy the most striking aspect of the law is that for the use of many intrusive investigative methods, a reasonable suspicion is no longer necessary.

5.7.9 Data Retention Directive (2006/24/EC)

Since traffic data plays a vital role in criminal investigations, law enforcement agencies have been pushing for mandatory data retention in Europe for quite some time. However, data retention has met with stiff resistance. Opponents of data retention argue that it poses a serious threat to privacy and liberty, and that mandatory data retention for the purposes of disciplinary surveillance is disproportionate. Moreover, they argue that data retention is ineffective and brings with it enormous costs. As a result the legislative process of the data retention directive has been slow.

---

28 Parliamentary Series II, 30 164.

However, the terrorist attacks in Madrid and London have sped up the legislative process and in September 2005 the European Commission adopted a proposal for a Data Retention Directive.[29] The goal of the Data Retention Directive is to harmonise the obligations on providers of publicly available electronic communications, or a public telecommunications network, to retain data related to mobile and fixed telephony for a period of one year, and internet communication data, for six months. The directive is not concerned with the content of the retained data.

The European Parliament adopted the directive on December 14, 2005, and the Ministers at the Justice and Home Affairs Council adopted it on February 21, 2006, thereby completing the official process leading up to an adoption of the directive. The Directive was adopted on March 15, 2006. Member States must bring the Directive into force by September 15, 2007. As such, data retention is not yet a part of Dutch Criminal procedure.

5.8 National security and privacy in the Netherlands

Software agents can contribute to a better intelligence position and therefore their use is especially considered in the area of national security. While international cooperation in the field of anti-terrorism is being undertaken in Europe, national security remains the cornerstone of state sovereignty, and as such it is still a predominantly national affair (Koops 2004, p. 177). Therefore, I shall discuss the law with regard to national security in the Netherlands and only focus briefly on the European context.

5.8.1 The European context

While there is no communitarian legislation that governs the workings of the European intelligence community, the intelligence services of the member states do cooperate in the field of anti-terrorism. In the area relevant to the subject matter of this thesis, *viz.* agent-enabled surveillance, a proposal made in February of 2000 by Portugal in the Working Party on Terrorism is particularly relevant.[30] The Portuguese presidency proposed to create a system that would facilitate the automated exchange of intelligence information between the intelligence services of the member states (Koops 2004, p. 185). At the basis of this system was a system of internet surveillance. Based on certain keywords generally associated with (cyber)terrorism operatives would scan the internet for suspicious websites and other content. Any relevant information found

29 Directive 2006/24/EC.

30 Portuguese Presidency, System for the exchange of information collection on the internet, document 5724/00 ENFOPOL 6, Brussels, February 4, 2000.

on the basis of the keyword searches would then automatically be relayed to other European intelligence services. However, up until now apprehension with regard to the mutual sharing of data has kept the intelligence services from implementing such a system. While the proposal itself is probably dead - it has not been discussed in over four years- it does illustrate the way in which internet surveillance and automated information exchange between the intelligence services might take shape in the future. Moreover, it illustrates the potential role of agent technology.

5.8.2 The General Intelligence and Security Service (AIVD)

Up until 2002 there was no clear legislation that regulated the use of surveillance powers by the Dutch intelligence community. That situation changed in February of 2002 when the *Wet op de Inlichtingen en Veiligheidsdiensten* (WIV) was enacted.[31] The act governs the operation of the two main Dutch intelligence services: the general intelligence service, the *Algemene Inlichtingen en Veiligheidsdienst* (AIVD) and the military intelligence service, the *Militaire Inlichtingen- en Veiligiheidsdienst* (MID). I shall limit myself to a short discussion of the investigative powers of the AIVD.

The AIVD is commissioned with the protection of national security in the Netherlands. To this end the AIVD, like any intelligence service, has far-reaching surveillance powers. In order to restrict the uncontrolled use of these investigative powers, the WIV sets forth certain rules regarding their application. Articles 20 through 30 WIV govern the application of investigative powers by the AIVD. In short, the rules set forth that the investigative powers of the AIVD may only be used when (Koops 2004, p. 2004):

- they are needed for the purpose of an investigation into people or organisations who pose a threat to democratic society, for the protection of national security or other important state interests, and for certain topics regarding other countries (article 18 WIV);
- approved by the Minister of the Interior (article 19 WIV);
- the demands of proportionality and subsidiarity are met (article 31-32 WIV);
- a record of the surveillance is kept (article 33 WIV).

Moreover, article 9 WIV stipulates that the AIVD may not conduct criminal investigations. Therefore, while intelligence information may to some extent be used in criminal investigations, it is in large parts inadmissible as evidence

31 *Staatsblad* 2002, 148.

in a trial.[32] This provision ensures that investigative powers granted to the AIVD for the protection of national security are not used in ordinary criminal investigations.

At the time of writing a bill is being proposed that would further strengthen the investigative powers of the AIVD.[33] The bill will give the AIVD greater authority when it comes to gathering data from a variety of sources for the purpose of data mining.

5.9 Criminal procedure and privacy in the United States

In this section I shall continue the discussion of the constitutional protection of privacy, but will focus more on the codification of this constitutional protection in criminal procedure. In the United States the constitutional protection of privacy is guaranteed mainly by the Fourth Amendment. Special attention will be devoted to the United States Patriot Act as it has fundamentally changed the rules governing surveillance in criminal procedures. While the *raison d'etre* of the Patriot Act is the fight against international terrorism, its provisions are so broad that they also include criminal investigations. Therefore, I shall start the discussion of the Patriot Act in this section and not in section 5.10 that deals with national security.

Before we turn to a discussion on the rules of criminal procedure, I shall first briefly discuss the Privacy Act of 1974, as it sets forth important rules for the use of (personal) data by agencies of the United States government.

5.9.1 Privacy Act of 1974

In 1974, Congress passed *The Privacy Act*, in part due to government violations of privacy during the Nixon administration.[34] The Privacy Act regulates the use and disclosure of personal data by government agencies. It is codified in Title 5, paragraph 552a of The United States Code. Much like the Dutch Data Protection laws it is inspired by the fair information practice principles. In 1988, the Privacy Act was amended by the Computer Matching and Privacy Protection Act, which governed the use of automated computer matching programs, such as data mining programs. The goals were to create procedural

32 In September of 2006 a ruling by the Dutch Supreme Court (Hoge Raad) opened up more room for the use of intelligence information in criminal trials (Hoge Raad, 01423/05, LJN AV4144). Moreover, in November 2006 legislation was passed that allowed the use of anonymous witnesses in criminal trials (Wet Afgeschermde Getuigen).

33 Tweede Kamer, vergaderjaar 2005–2006, 30 553, nr. 2.

34 Pub. L. No. 93-579, 88 Stat. 1897 (1974).

uniformity in the application of matching programs, a greater degree of oversight, and the insurance of the data subject's rights.

While the Privacy Act sets forth important rules for data processing by the government, most notably in the area of data mining, its impact on law enforcement is minimal in practice. The reason for this is that the Privacy Acts contains a number of provisions that exempt law enforcement agencies from the rules of the Privacy Act. Federal law enforcement can thus bypass the rules of the Privacy Act when it comes to the use of information gathering and data-mining technologies such as software agents.

5.9.2 Title 18 USC, Crimes and Criminal Procedure

Title 18 of the United States Code governs crime and criminal procedure in the United States. The use of electronic surveillance tools is not exhaustively codified in the United States Code. As described in the sections on the constitutional protection of privacy, the question whether a particular surveillance practice is constitutional, is most often a matter that is decided by the courts on the basis of the Fourth Amendment. However, some parts of the United States Code do deal with surveillance and privacy in criminal procedures. With regard to restrictions to the federal government's ability to conduct electronic surveillance, various important laws have been enacted over the years. For the subject matter of this thesis, Title III of the *Omnibus Crime Control and Safe Streets Act of 1968* and the *Electronics Communications Privacy Act of 1986* are most relevant.

The Omnibus Crime Control and Safe Streets Act of 1968
In 1968, the *Omnibus Crime Control and Safe Streets Act* was enacted.[35] Title III of the Omnibus Act created a legal foundation for electronic surveillance in the United States. The Act prohibited private persons to conduct electronic surveillance, while granting law enforcement officials the authority to conduct electronic surveillance. More specifically, Title III authorised the interception of wire and oral communications by federal agents for the purpose of a criminal investigation. The term interception refers to the acquisition of the contents of any wire, electronic, or oral communication transmitted from one party to another.

Title III has been entered into the United States Code under chapter 119 (§§ 2510 *et seq*.) and has been updated several times in order to keep up with the state of technology. The most important change to the statute came with the Electronic Communications Privacy Act.

35 Pub. L. No. 90-351, 82 Stat. 212 (1968).

The Electronic Communications Privacy Act of 1986
As a result of developments in information and communication technologies, Congress enacted the Electronic Communications Privacy Act in 1986.[36] The Act amended the Omnibus Crime Control and Safe Streets Act, broadening its scope to include electronic communications (such as email, data transmissions, and faxes).

While interception is concerned with the acquisition of the content of communication, the acquisition of dialing and signalling information can be equally important. Therefore, the Electronic Communications Privacy Act also provided a statutory basis for the use of pen registers and trap and trace devices, which enabled law enforcement agencies to collect non-content traffic information associated with telecommunications (18 USC, chapter 206, § 3121 *et seq.*). A pen register is a surveillance device that captures the numbers of outgoing telephone calls, while trap and trace devices capture the numbers identifying incoming calls. These devices do not collect any information regarding the content of telephone calls. Unsurprisingly, pen registers and trap and trace devices have become important investigative tools in the information age.

5.9.3 The Attorney General's Guidelines

The rules and procedures for conducting criminal investigations that the Federal Bureau of Investigation (FBI) has to follow are further specified in *The Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigation* (DOJ 2002). These Guidelines were supplemented by the *Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (Minow *et al.* 2002, p. 29).[37]

5.9.4 The United States Patriot Act

On October 11, 2001 new anti-terrorism legislation passed the Senate in response to the September 11 terrorist attacks. The legislation, that carried the short title 'USA Patriot Act', updated and amended over 15 different laws in order to provide more adequate legal tools to combat terrorism. Amongst other things it created new crimes, new penalties, and new procedural efficiencies for use against domestic and international terrorists. Moreover, it gave greater authority to public officials to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes (Doyle 2002).

---

36 Pub. L. No. 99- 508, 100 Stat. 1848 (1986).

37 In the context of intelligence gathering for national security the rules and procedures are specified in President Reagan's *Executive Order 12333*.

When enacted in 2001, the Patriot Act gave sweeping new authorities to law enforcement agencies to collect and share information regarding possible terrorist attacks. Many of these new powers were considered to be so far-reaching that they contained a 'sunset clause'. This clause limited the time that certain provisions would be in effect to December 31, 2005. At the end of 2005 the Bush administration sought to renew the Patriot Act without any significant reforms, this included an extension of the controversial sections that contained sunset clauses. While initially resistance to an extension of certain parts of the Patriot Act was strong, Congress eventually passed the renewal in March 2006 after some privacy safeguards were added.[38] However, most of the controversial clauses that were to sunset at the end of 2005 were extended without significant changes.

For the subject matter of this thesis Title II of the Patriot Act is of particular interest as it deals with information sharing and investigative powers. Title II reflects three themes: (1) expanded investigative and surveillance authority, (2) expanded investigative and surveillance abilities, and (3) information sharing of 'foreign intelligence' information between federal investigative agencies, in particular the FBI and CIA (Michaels 2002, p. 46). Below I shall describe those provisions most relevant to the subject matter of this thesis.

Information sharing (sec. 203)
In order to make the sharing of information more easy, the Patriot Act amends section 2517 of title 18 of the United States Code. Section 203 of the Patriot Act allows any investigative officer, law enforcement officer, or attorney of the government to disclose knowledge of any wire, oral, or electronic communication (or evidence derived therefrom), to any other federal law enforcement, intelligence, protective, immigration, national defence, or national security official, to assist these officials in the performance of their official duties (§b). The information that may be shared includes foreign intelligence and foreign intelligence information (§d). While paragraphs (b) and (d) were set to sunset on December 31, 2005, they have been extended through the Patriot Reauthorization Act.

Pen registers and trap and trace devices (sec. 216)
Section 216 of the USA Patriot Act updated the existing legislation dealing with trap and trace devices in two important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to trace communications on the internet and computer networks, and (2) pen/trap orders issued by federal courts now have nationwide effect (Schmalleger 2004, p. 314). Furthermore, section 216 provides that upon certification that the information likely to be obtained from the installation of the pen/trap is relevant to an ongoing criminal investigation, a federal court shall enter an *ex parte* order authorizing

38 USA PATRIOT Improvement and Reauthorization Act of 2005, HR 3199.

the use of the pen trap/register. The surveillance can be aimed at any foreign national, but may also be aimed at United States citizens if the activity the citizen is involved in is not under the protection of the First Amendment (Michaels 2002, p. 58). This section was also set to sunset at the end of 2005, but has been extended through the Patriot Reauthorization Act.

5.10 National security and privacy in the United States

Investigations for the purpose of gathering foreign intelligence give rise to a tension between the Government's legitimate national security interests and the protection of privacy interests (Bazan 2004, p. 7). Traditionally, law enforcement and national security were two discrete areas with different rules of procedure. However, with the advent of the Patriot Act, the line between criminal investigations and investigations into terrorist activities has become increasingly vague. This is due to the vague description of terrorism and terrorist activities in the Patriot Act, and as we have seen in the previous section, due to provisions that enable law enforcement agencies and intelligence agencies (most notably the CIA) to share data extensively.

5.10.1 Title 50 USC, War and National Defense

Title 50 of the United States Code deals with the issue of war and national defense. The latter includes intelligence activities and is thus of particular interest to the subject matter of this thesis. The title was significantly revised in the wake of the September 11 terrorist attacks.

Title 50 USC, Chapter 36, § 1801 et seq.
The Foreign Intelligence and Surveillance Act (FISA), which was passed in 1978 in order to provide a statutory framework for the use of electronic surveillance in the context of foreign intelligence gathering, makes up an important part of Title 50 USC. By enacting the FISA, Congress sought to strike a balance between national security interests and personal privacy rights (Bazan 2004, p. 2). The FISA was initially limited to electronic eavesdropping and wiretapping but was amended in 1994 and 1998 to permit covert physical entries and pen/trap orders.

The FISA is specifically aimed at the collection of foreign intelligence information, which is information that relates to the United States ability to protect against (1) possible hostile acts of a foreign power or an agent thereof, (2) sabotage or terrorism by a foreign power or agent thereof, and (3) covert intelligence activities by a foreign power or agent thereof (50 U.S.C. 1801(e)). The FISA relaxes some of the constitutional limitations to conducting surveillance, most notably the protection provided by the Fourth Amendment.

Under the Fourth Amendment, a search warrant must be based on a probable cause; this is not the general rule under the FISA: surveillance under the FISA is permitted based on a finding of a probable cause that the target is a foreign power or an agent thereof, there is no need to establish whether the target is actually engaged in criminal activity.

Because of the inherent dangers to privacy and individual liberty present in the FISA, the use of the FISA has certain limitations. First of all, the application of the FISA is limited to foreign intelligence information, as such investigative powers granted by the FISA may not be aimed at United States citizens unless there is a probable cause to believe that their activities may involve espionage or other similar conduct. Second, the FISA has a 'minimisation requirement' designed to prevent the power of foreign intelligence gathering from being used for routine criminal investigations. While courts do allow FISA-obtained information to be used in criminal trials, the minimisation requirement mandates that procedures must be implemented to minimise the collection, retention, and dissemination of information about United States citizens.

5.10.2 The United States Patriot Act

While the United States Patriot Act is aimed at combating terrorism, we have seen that some of its provision can also be used over the course of a normal criminal investigation. Still, the most important parts of the Patriot Act are aimed at updating and amending the FISA. I shall discuss two provisions that are of particular interest to the subject matter of this thesis.

Roving wiretaps (sec. 206)
The Patriot Act amended the FISA to allow court orders permitting so-called multipoint electronic surveillance or 'roving wiretaps'. In the case of multipoint electronic surveillance, the court order does not require particularity with respect to the identification of the instrument, place, or facility to be intercepted, when a court finds that the actions of the target of the surveillance are likely to thwart such identification. While roving wiretaps were already available in normal criminal investigations, this investigative power granted by section 206, relaxed many of the requirements stipulated in the context of a normal criminal investigation. For instance, orders issued under section 206, 1) use a lower legal standard than the probable cause used in criminal investigations, 2) are subject to less judicial oversight, and 3) can last longer (up to a year) than those issued for the purpose of a criminal investigation. Moreover, section 206 stated that it was not necessary to identify the target of the roving wiretap. In practice, this established the authority to tap every house or office that the suspect had visited, for up to a year on the basis of a single warrant, without the necessity to identify the suspect. This practice came to be known as a 'John Doe' wiretap.

Section 206 was to sunset at the end of 2005 but was extended through the Patriot Reauthorization Act. While the authority to conduct multipoint electronic surveillance remained, the Patriot Reauthorization Act did introduce new procedural requirements. For instance, it is now necessary to identify the specific target of a multipoint electronic surveillance, limiting the room for 'John Doe' wiretaps.

Access to records and other items under the FISA (sec. 215)
One of the most controversial sections of the original Patriot Act was section 215. This section allowed federal agents to order secretly a third party to turn over business, medical, library and other records as well as 'tangible things' for the purpose of an investigation under the FISA. The demands for records were accompanied by a 'gag order' prohibiting the recipient from telling anyone that they received a Section 215 order. Section 215 was also due to sunset at the end of 2005. The Patriot Reauthorization Act extended the sunset period to 2009. Moreover, section 215 was amended in order to reduce the risks to privacy and individual liberty. Changes to section 215 included better judicial oversight and a new requirement for stating a 'reasonable ground' for obtaining tangible things. However, as a whole section 215 with its sweeping authority to obtain records and tangible things secretly, remains a highly controversial piece of legislation.

5.10.3 Legislation concerning Terrorist Surveillance Programs

In 2002 President Bush authorised the National Security Agency (NSA) through a secret executive order to wiretap phone and email communications of United States persons within the United States, without obtaining a warrant or court order. The existence of the program (called a Terrorist Surveillance Program or TSP) was disclosed by the press in December 2005 and subsequently acknowledged by the White House.

In an effort to stop the secret program, the American Civil Liberties Union (ACLU) challenged its constitutionality before the District Court of Michigan. The District Court ruled that the NSA program constituted a violation of the First and Fourth Amendment, the separation of powers doctrine, and the FISA.[39] However, since the case has not yet been brought before the Supreme Court, it is too early to determine whether the ruling of the District Court will be upheld.

Moreover, two pieces of legislation were introduced aimed at legalising the NSA program and any other Terrorist Surveillance Programs. The first piece

39 American Civil Liberties Union, *et al.* v. National Security Agency, *et al.*, U.S. District Court for the Eastern District of Michigan, D.C. No. 06-CV-10204.

of proposed legislation is the *Terrorist Surveillance Act of 2006*.[40] This act allows the President to authorise a TSP without a court order for a period of up to 45 days if: (1) the President determines that such a progamme is necessary to protect the United States, its citizens, or its interests, (2) there is probable cause to believe that a surveillance subject is an agent or member of an organisation designated on a special 'Terrorist Surveillance List', (3) the surveillance is initiated and conducted in a manner reasonably designed to acquire only communications to or from the United States where at least one the surveillance subjects is located outside the United States, or the communications appear to originate or terminate outside the United States; (4) there is not a substantial likelihood that the surveillance will acquire the substance of any communication where every party thereto is located within the United States; and (5) procedures are in place for the minimisation of privacy infringements.

The second piece of proposed legislation is the *Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006.* The goal of this bill is to change the FISA provisions concerning electronic surveillance to: (1) extend the period for the application for orders for emergency electronic surveillance, (2) permit the Attorney General to delegate authority to approve electronic surveillance applications, and (3) authorise the Attorney General to appoint personnel within the FBI and NSA to authorise emergency surveillance.

At the time of writing this thesis the two pieces of legislation passed the Senate Committee on the Judiciary and were placed on the agenda of the Senate. But since they were not passed before the end of the 109th session of Congress, they were cleared from the books and thus never became law. As of yet it is uncertain whether the bills will reemerge in some form in the next session of Congress.

5.11 THE DIFFERENT PHASES IN AN INVESTIGATION

In the previous sections we examined the legal requirements for the use of various investigative powers in the Netherlands and the United States. What we must also take into account in judging whether the use of (electronic) surveillance is authorised, is the phase in which the investigation is in.

40 *Terrorist Surveillance Act of 2006*, S. 2455, 109th U.S. Congress (2005-2006); *Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006* , S. 3001, 109th U.S. Congress (2005-2006).

5.11.1 The Netherlands

In Dutch criminal law we can distinguish the following three phases in an investigation: (1) the gathering of information to maintain a general level of intelligence, (2) the exploratory investigation, and (3) the 'normal' criminal investigation (Sietsma *et al.* 2002, p. 34).

General information gathering
Law enforcement agencies need to maintain a certain level of intelligence in order to execute the task of law enforcement, and to this end they may conduct surveillance. While many of the investigative powers that may be used in a criminal investigation are codified within the rules of criminal procedure, there is no exhaustive list of surveillance methods that may be used for general intelligence gathering in the Netherlands. The authority to conduct surveillance in order to execute the normal police task can be derived from article 2 of the Police Act of 1993. The determining factor in deciding what investigative methods may be used in the execution of the normal police task is that the impact the investigative method has on the privacy of individuals.

The exploratory investigation[41]
In order to combat serious forms of crime in certain sectors, law enforcement may conduct an exploratory investigation prior to an actual criminal investigation. An exploratory investigation covers the gathering and further processing of data from police and other records. Exploratory investigations are not investigations and as such investigative powers may not be applied. The rules concerning the exploratory investigation are codified in article 126gg CCP.

Criminal investigation
Article 132a CCP defines the term 'criminal investigation' in the Dutch criminal procedure. The article states the following:

> "A criminal investigation is an investigation headed by the public prosecutor for the purpose of taking decisions in a criminal procedure. A criminal investigation must be based on the reasonable suspicion that a crime has been committed or crimes described in article 67 paragraph 1 CCP are being planned or perpetrated in association that, considering their nature or their connection to other crimes planned or perpetrated in association, constitute a serious threat to law and order."

When a criminal investigation has been started, coercive measures and investigative powers may be used, provided they are used in compliance with the rules of criminal procedure.

41 The exploratory investigation, verkennend onderzoek in Dutch, is also oftentimes translated as the phenomenon investigation.

When it comes to aiming a criminal investigation against a criminal organisation (including terrorist organisations) investigative powers may be used pro-actively. The investigative powers that may be used to gather information and evidence against a criminal organisation pro-actively are governed by a special Title in the law of criminal procedure.

5.11.2 The United States

In the United States we can distinguish three different phases in an investigation too. The *Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations* (DOJ 2002) describes these various phases. It distinguishes between the checking of leads, the preliminary inquiry, and the full criminal investigation.

Checking of leads
The lowest level of investigative activity is the prompt and extremely limited checking out of initial leads. The checking of leads is undertaken whenever information is received of such a nature that some follow-up as to the possibility of criminal activity is warranted (DOJ 2002, p. 2). This limited form of investigative activity is conducted with an eye toward promptly determining whether further investigation (either a preliminary inquiry or a full investigation) should be conducted.

The preliminary inquiry
A preliminary inquiry is undertaken when there is information or an allegation which indicates the possibility of criminal activity and whose responsible handling requires some further scrutiny beyond checking initial leads. This authority allows federal agents to respond to information that is ambiguous or incomplete (DOJ 2002, p. 2). In this stage far-reaching investigative techniques may already be used, including running informants and conducting undercover activities. However, the use of electronic surveillance in this phase is explicitly prohibited.

Full investigations
We can distinguish between two types of full investigations: general crimes investigations and criminal intelligence investigations. Whether a general crimes investigation can be initiated or a criminal intelligence investigation depends on the information and the investigative focus. A general crimes investigation may be initiated where facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed. Preventing future criminal activity, as well as solving and prosecuting crimes that have already occurred, is an explicitly authorised objective of general crimes investigations (DOJ 2002, p. 2). Furthermore, under the Guidelines a general crimes investiga-

tion is also allowed when there is not yet a current substantive or preparatory crime, but where facts or circumstances reasonably indicate that such a crime will occur in the future.

The second type of full investigation authorized under the Guidelines is the criminal intelligence investigation. The focus of criminal intelligence investigations is the group or enterprise, rather than just individual participants and specific acts. The immediate purpose of a criminal intelligence investigation is to obtain information concerning the nature and structure of the enterprise (including information relating to the group's membership, finances, geographical dimensions, past and future activities, and goals) with a view toward detecting, preventing, and prosecuting the enterprise's criminal activities (DOJ 2002, p. 2). A criminal intelligence investigation is warranted in two instances: investigations into racketeering enterprises and investigations into terrorism enterprises.

5.12 General remarks on substantive criminal law

Up until now I have discussed the law of criminal procedure and its relation to privacy. One final issue that deserves mention in this chapter however, are the changes that have been made to substantive criminal law in both the United States and the Netherlands over the past years. These changes are predominantly a response to the threat of international terrorism. To a lesser degree they can be contributed to the growth of organised crime. I shall only describe the general direction in which substantive law has developed over these past years, since it is beyond the scope of this thesis to explore fully the changes made to substantive criminal law.

When we view the changes to substantive law in both the United States and the Netherlands we can establish that the scope of criminal liability has been greatly expanded over the past few years. This is due to the fact that there is a general trend towards increased penalisation of actions in preparation of a terrorist attack, and a broadening of the definition of terrorism in criminal law.

Changes to substantive law are deemed necessary because of the severity and societal impact of terrorist attacks. By expanding criminal liability to the preparatory phase, the legislator hopes to enable intelligence and law enforcement agencies to apprehend and convict suspected terrorists in an earlier stage, *viz.* before they can execute their plans. While in itself this is a noble goal, possible negative consequences of this development should not be disregarded. A possible negative effect of increased criminal liability is the shift from a system of criminal law that is based around the actual criminal act itself, towards a system that is based more on the intention to commit a crime (Moerings 2006, p. 168).

With the changes in substantive criminal law, investigative powers such as electronic surveillance can be used to detect suspicious behaviour in an earlier stage. Moreover, due to broad definitions of terrorism more intrusive surveillance measures may be used in an investigation.

5.13 RISK JUSTICE

The desire for risk-management and security in society has had a significant influence on the development of criminal law in recent years. It could be said that we are moving towards a system of 'risk justice' (Moerings 2006, p. 168). In such a system the focus is not on solving crime and the legal punishment of criminal offences, but rather on the prevention of criminal offences and the reduction of risk. In both substantive criminal law and the law of criminal procedure we can clearly discern the development of risk justice. In the substantive criminal law of both the Netherlands and the United States we can see that the scope of criminal liability has been greatly expanded over the past years, most notably in the area of terrorism. In particular, the expansion of criminal liability to include preparatory acts and conspiracies to commit terrorist offences is noteworthy. The increased criminal liability creates a 'gray area' in the law, between merely thinking about a criminal act and actually committing one, where sweeping investigative powers may be used nonetheless. This increased scope of criminal liability forms a radical departure from traditional criminal law. The change that has been brought about by this development is that it is no longer just the actual criminal *act* that is punishable, but now also the *thought* of a criminal has become punishable (Moerings 2006, p. 168). It is clear that this situation can lead to mistakes and arbitrary decisions by law enforcement agencies that could threaten the privacy and liberty of individuals.

5.14 Provisional conclusion

In this chapter I explored the illusive concept of privacy. Since privacy is so difficult to define, I opted to describe various conceptions of privacy and the dimensions to which the right to privacy can apply. I also described how the right to privacy has developed over time to keep up with technological changes.

For the context of this thesis we see that the conception of privacy as limit to power is most relevant. The most direct example of the role privacy can play in limiting power is the Panopticon. In the Panopticon we see that a complete absence of privacy destroys personal autonomy. Through secrecy and concealment we can create a sphere of autonomy for ourselves thereby limiting the power of surveillance.

In chapter 3 I established that there is a definite trend towards more surveillance. In this chapter we have seen how privacy can limit the power of surveillance and regulate its use. Both in the common law and the civil law tradition we see that the right to privacy is seen as the primary bulwark against electronic surveillance. However, we have also seen in the sections on the law of criminal procedure and the section on substantive criminal law, that in response to the threat of international terrorism, new legislation is adopted that sanctions the extensive use of electronic surveillance.

Given these prior considerations, it is questionable whether the right to privacy is an ideal candidate when it comes to securing (individual) liberty. In order to determine whether the conception of privacy as limit to power is useful we must first gain a greater understanding of the relation between privacy and liberty.

6 Privacy and liberty

The erosion of freedom rarely comes as an all-out frontal assault. Rather, it is a gradual, noxious creeping cloaked in secrecy and glossed over by reassurances of greater security.
Senator Robert C. Byrd

Surveillance is not a goal in itself, but rather a means to an end. In general, surveillance methods are employed to enable a greater deal of control over a process, area, situation, or person. With regard to persons, surveillance can be described as the collection and processing of personal data, whether identifiable or not, for the purpose of influencing or managing those, whose data have been garnered (Lyon 2001, p. 2). The 'natural' opposite of control is not privacy but rather freedom or liberty.[1] I will argue that in the information society the right to privacy is primarily aimed at preventing certain parties from gaining too much knowledge about us, effectively turning privacy into an issue of liberty or, more broadly speaking, an issue of power.

In section 6.1 I shall explore the conception of privacy as limit to power that was put forward in chapter 5 more in depth. In section 6.2 I introduce two different concepts of liberty put forth by Berlin and determine their relationship to the right to privacy in section 6.3. In section 6.4 I shall discuss some of the limitations the right to privacy has when it comes to the complete protection of individual liberty. I shall conclude this chapter by summarising the arguments in section 6.5.

6.1 The conception of privacy as limit to power

An important conceptualisation of privacy -especially in this age of high-tech surveillance- is privacy as a limit to power. Since knowledge is power, any measure that can reduce the accumulation of information will limit the power that can be exercised by those who control the information. The right to privacy, i.e., the right to prevent access to the personal sphere, can fulfil this function. This particular conceptualisation of privacy is based on what Solove (2004b, p. 8) describes as the 'secrecy paradigm'. Privacy is invaded by un-

1 In this thesis the notions of freedom and liberty have roughly the same meaning. Therefore I use both words interchangeably.

covering one's hidden world, by surveillance, and by the disclosure of concealed information. The harm these invasions may cause are: inhibition, self-censorship (i.e., Panoptic effects), embarrassment, and damage to one's reputation (Solove 2004b, p. 8).[2] By ensuring an individual's right to privacy, these harmful effects can be negated, as access to the private sphere without prior permission is deemed illegal.

With the advent of information and communication technology the need to regulate the use of personal data became greater. An important goal of data protection is to limit the accumulation of extensive digital dossiers that can be used to influence or control a data subject. This is reflected clearly for instance in article 1, paragraph 1 of the European Data Protection Directive (95/46/EC):

> "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

It is beyond question that the conception of privacy as limit to power plays an important role in the idea of informational privacy. If we look at the current use and interpretation of the right to (informational) privacy, it almost seems as if that the right to privacy has become the sole means of protection against attacks on individual liberty in the information society. Especially when it comes to the protection of personal data, the primary motivation to invoke the right to privacy seems to be to limit the power of third parties. From a narrowly defined right to the respect for a private sphere, the right to privacy has been transformed into an all-encompassing value aimed at safeguarding both privacy *and* liberty (Blok 2002, p. 120). Privacy has thus become a preferred way in which to address power asymmetries between the observers and the observed (Dubbeld 2004, p. 188).

This transformation has brought about a confusion of tongues, because privacy and liberty have developed into values without a clear distinction. It is questionable whether both privacy and liberty have gained much from the transformation of privacy. To analyse these matters we formulate the following question: why should we make a distinction between privacy and liberty when dealing with software agents and control?

One could argue that the right to (informational) privacy provides ample protection for both privacy and liberty. As such, making a distinction between the right to privacy and the right to liberty merely for the sake of argument would be of little to no consequence to everyday reality, where the right to

2 In the case of *ACLU vs. NSA* for instance, plaintiffs (i.e., the persons being wiretapped by the NSA) claimed that the NSA wiretaps had a chilling effect on their behaviour. See: American Civil Liberties Union vs. National Security Agency, United States District Court, Eastern District of Michigan, Southern Division, case no. 06-CV-10204.

privacy adequately performs its different functions. However, in my opinion we must make a distinction. While privacy certainly plays an important role in safeguarding liberty, I believe that the right to privacy cannot by itself supply the necessary protection against excessive control or coercion made possible by the use of (personal) data. In almost every democratic, constitutional state, a broad constellation of human rights combined with a system of checks and balances guarantees the maximum amount of liberty and security possible for the state's subjects. I believe it is unwise, if not impossible, to replace such intricate systems of constitutional rights with a singular right to privacy when dealing with (individual) liberty.

6.2 TWO CONCEPTS OF LIBERTY

In order to make any relevant claims about privacy and liberty, we must first take a closer look at their relationship. To shed some light on the situation I shall discuss the relationship between both ideas using the two concepts of liberty put forth by Berlin in his classic, thought-provoking essay *Two Concepts of Liberty* (Berlin 1958, p. 166-218). Although subsequent scholars have interpreted, adapted, and criticised Berlin's framework, I still find his classic distinction useful because it allows me to illustrate more clearly the different aspects of liberty and their relation to privacy.[3]

The first concept of liberty that Berlin identifies is that of 'negative liberty'. In this sense liberty, is the area within which an individual can act unobstructed by others. The concept of negative liberty deals with the question what the area is within which the subject -a person or group of persons- is or should be left to do or be what he is able to do or be, without interference by other persons (Berlin 1958, p. 169). In other words, negative liberty is freedom *from.*

As second concept of liberty Berlin puts forward 'positive liberty'. It is derived from the wish on the part of the individual to be his own master. Or as Berlin (1958, p. 178) so eloquently puts it:

> "I wish my life and decisions to depend on myself, not on external forces of whatever kind. I wish to be the instrument of my own, not of other men's act of will. I wish to be a subject not an object; to be moved by reasons, conscious purposes, which are my own, not by causes which affect me, as it were, from outside. I wish to be somebody not nobody; a doer – deciding, not being decided for, self-directed and not acted upon by external nature or by other men as if I were a thing, or an animal, or a slave incapable of playing a human role, that is, of conceiving goals and policies of my own and realising them. This is at least part of what I mean when I say that I am rational, and that is my reason that distinguishes me

3 See for instance: MacCallum (1967), Christman (1991), and Skinner (1998).

> as a human being from the rest of the world. I wish above all to be conscious of myself as a thinking, willing, active being, bearing responsibility for my choices and able to explain them by reference to my own ideas and purposes. I feel free to the degree that I believe this to be true, and enslaved to the degree that I am made to realise that it is not."

Positive liberty is thus not freedom *from*, but freedom *to*. It is the ability on the part of the individual to determine for himself his own course of action. Positive liberty can be seen as a form of self-coercion, which sees the attainment of liberty in the terms of self-fulfilment: I wish to become the kind of person that I know I have it in myself to be (McClellan 1996, p. 265). In other words, positive liberty is not necessarily the *absence* of something (obstacles, barriers, and interference), but rather the *presence* of something (self-determination, self-realisation, self-control). In other words I am free to the extent that I can make up my own mind about how I choose to live my life and enslaved to the degree that it is not me but others who make up my mind. The concept of positive liberty is primarily concerned with the question "What, or who, is the source of control or interference that can determine someone to do, or be, this rather than that?" (Berlin 1958, p. 169)

As Berlin points out himself, the freedom which consists in being one's own master, and the freedom which consists in not being prevented from choosing as I do by other men, may seem to be no more than positive and negative ways of saying the same thing (Berlin 1958, p. 178). However, both concepts of liberty have developed along clearly distinct paths and have even come into direct conflict with each other, as I shall describe in the section on positive liberty. My reason for using the two concepts of liberty is that they are useful for defining the concept of liberty and can help clarify the subtle difference between the mere absence of constraints or interference (negative liberty) and the freedom from coercion or manipulation by a third party. In the next two sections I shall therefore study the two concepts of liberty somewhat more in depth. Emphasis will be placed on the concept of negative liberty (especially its origins), because it is has the most obvious connection with the right to privacy.

6.2.1 The concept of negative liberty

The origins of the concept of negative liberty can be traced back to the Enlightenment and the rise of individualism. Kant characterised the Enlightenment as man's release from self-incurred tutelage (Foucault 1997, p. 7). During the Enlightenment, the natural sciences and the aftermath of bitter religious strife during the Reformation, would spark a new intellectual movement that challenged tradition, religious dogma and authority as the basis of knowledge. Empiricism (with protagonists such as Bacon, Locke, and Hume) and rationalism (with protagonists like Descartes and Leibniz) would form

the foundations of modern science, which was to be applied to every conceivable field of inquiry, including political thought. In enlightened political thought liberty, equality, justice, individuality, and limitations on government power would become predominant themes that still feature prominently today. Many great thinkers such as Hobbes, Hume, Rousseau, and Montesqieu developed political theories during the Enlightenment. However, if we take the subject matter of this thesis into consideration, the work of John Locke is probably most relevant, so I will focus a little more on his work.

In his *First Treatise of Government,* a reaction to Filmer's (1680) *Patriarcha*, Locke (1690) rejects Filmer's argument that all kings rule by divine right. In his *Second Treatise of Government,* Locke argues that instead of a divine right, the authority of any government is based on the idea of a 'social contract' between equal individuals (Hampsher-Monk 1992, p. 81). Locke argues that the natural state of mankind is that of perfect freedom to order their actions and dispose of their possessions and persons as they think fit within the bounds of the law of nature (Locke 1690, p. 287). In his view, liberty and equality were part of the 'state of nature' as imposed by God. Through his theory of private property, arguing that every person has a property in his own person (Locke 1690, p. 304), Locke acknowledged the individuality and equality of man and the existence of inalienable, fundamental human rights (Hampsher-Monk 1992, p. 88). Locke uses these arguments to address the issue of limitations to government powers. While Locke saw government as a product of the social contract and a necessary means to protect private interests of individuals in society, in the eyes of Locke the authority of government was not absolute. For Locke, the most important aspect in judging whether a government (not necessarily a democracy) is legitimate, is the degree of power it claims over individuals, for Locke legitimate power is power plus right (Hampsher-Monk 1992, p. 103).

Locke's seminal writings and that of his contemporaries on political thought would form the basis for modern (liberal) democratic theory. Over the course of some hundred years enlightened political thought would find its way, either gradually or through revolution, into almost every state in the western hemisphere.

About a hundred seventy years later, Mill, a great champion of liberty, wrote a highly influential essay that is also of particular interest to the subject matter of this thesis. Whereas Locke applied his liberal ideas to government in general, Mill applied them to the principle of democracy. In his essay *On Liberty*, Mill argued that there is a limit to the legitimate interference of collective opinion with individual independence (Mill 1859, p. 91). If collective opinion were always to gain the upper hand against individual independence, our right to self-determination along with our individuality and human dignity would be diminished or even lost completely. The defence of liberty in this sense consists in the negative goal of warding off interference (Berlin 1958, p. 174).

We may conclude that the concept of negative liberty defines the area in which an individual is free from outside interference of any kind. In the concept of negative liberty there must exist a minimum area of personal freedom that must at no account be violated. It follows that a frontier must be drawn between the public and the private in order to secure this area of non-interference (Berlin 1958, p. 171).

6.2.2 The concept of positive liberty

Critics of the concept of negative liberty argue that the mere freedom to choose is in itself without any inherent moral quality and is as such both empty and arbitrary.[4] Not only critics of the concept of negative liberty feel this way, to some extent even the most rigorous proponent of negative liberty, Mill, acknowledged the fact that the only freedom which deserves the name, is that of pursuing our own good in our own way (Mill 1859, p. 97). Pursuing our own good involves making commitments, maintaining relationships, and keeping to our promises. For Berlin 'becoming our best' is the defining element of the concept of positive liberty. Becoming our best, however, is not something that comes along easily; it requires some form of self-mastery. Human beings are creatures divided against themselves: the 'higher', rational self must at times bring the 'lower' nature to heel, in order to pursue long-term goals and function properly within a society. In other words you must *force* yourself to be *free* (Hampsher-Monk 1992, p. 179).

For supporters of the concept of negative liberty, including Berlin himself, the idea that self-mastery is freedom, though sound in theory, is ultimately suspect. The concept of positive liberty provides us with a paradox: coercion, which disqualifies acts from being free, is necessary in order to attain freedom (McClellan 1996, p. 179). The concept of positive liberty becomes even more suspect when we conceive the self as wider than the individual. Then the concept of positive liberty bears with it the risk of authoritarianism (Carter 2003, p. 2). The coercion of individuals for their own sake, in order to bring them to a higher level of freedom, might be seen as a noble act, but as history has pointed out very clearly, it has also been the justification for some of the most brutal totalitarian regimes in the world.

The concept of positive liberty is therefore somewhat problematic. Scholars such as Christman (1991) have opted for a more individualistic approach to positive liberty. Christman argues that positive liberty is primarily concerned with the ways in which desires are formed, whether as a result of rational reflection on all the options available, or as a result of pressure, manipulation or ignorance (Carter 2003, p. 4). This interpretation of positive liberty is most

4 See, for instance, Taylor (1979).

interesting with regard to the subject matter of this thesis. Interpreting the concept of positive liberty in this way can help us clarify the difference between constraints (negative) and manipulation or coercion (positive).

6.3 Privacy and the two concepts of liberty

Now that we have discussed both concepts of liberty, we can turn our attention to the relationship between privacy and the two concepts of liberty.

6.3.1 Privacy and negative liberty

At the end of the 19th century, justices Warren and Brandeis (1890) made the first explicit reference to a right to privacy in their renowned article *The Right to Privacy: The Implicit Made Explicit*. Dismayed as they were by the practices of the gossip press which used "new inventions and business methods" to invade the "sacred precinct of private and domestic life", Warren and Brandeis set out to explore the possibility and origin of a right to privacy. Warren and Brandeis came to the conclusion that the right to privacy formed part of the inviolate personality and saw it as: "the next step that must be taken for the protection of the person, and for securing to the individual… …the right 'to be let alone'" (Warren, Brandeis 1890, p. 193). According to Warren and Brandeis the right to privacy was, much like the concept of negative liberty, a "right as against the world". From this definition and the section on negative liberty we may conclude that the right to privacy is deeply rooted in the idea of negative liberty. Privacy protects us from the observing gaze of others and enables us to hide certain elements of our behaviour or personality from outside scrutiny.

In chapter 5 we have established that with emergence of electronic record keeping two distinct lines of privacy theory developed. When we examine the concept of negative liberty we can associate it primarily with the privacy theory that is based on the traditional notions of the 'private sphere' and thus with secrecy and anonimity. When we observe the legal framework for the protection of privacy and the regulation of surveillance practice, we can establish that this line of privacy theory is dominant in the law of both the Netherlands and the United States. Thus, the current legal framework is primarily concerned with the protection of negative liberty.

Privacy forms a major element of negative liberty and it may even seem somehow logical to qualify negative liberty and privacy as roughly the same concept, the right 'to be let alone' so to speak. But while the right to privacy certainly plays a key role in safeguarding negative liberty, I believe that they are most certainly not the same concepts, and I do not feel privacy can offer the amount of protection required for negative liberty. Negative liberty is made

up of more elements than the sanctity of the home, corporeal privacy, or the right to keep certain information secret. Not every form of interference is by definition a violation of a private sphere and as such protected by the right to privacy. Negative liberty means freedom from as much interference as possible in a society, not just freedom from interference into a predefined private sphere. I believe it is safe to assume that not every violation of liberty constitutes a violation of privacy. If, for instance, I am physically constrained by a person from leaving or entering a certain area, my freedom is diminished while my (informational) privacy is not. When I am denied the freedom of religion or the right to protest my liberty is diminished while my privacy is not.

I believe that the right to privacy is therefore ill-suited for the *complete* protection of negative liberty in the information society because it relies, by definition, on a distinction between the public and the private. The right to privacy in the 'classic' sense protected a narrowly defined private sphere and while the scope of the right to privacy has broadened it still relies on this distinction between the public and the private sphere. When a violation of my freedom occurs that does not entail the violation of a 'private component' of my life (such as my house, correspondence, or personal information), the right to privacy cannot provide any protection. This means that certain important elements of negative liberty that do not have a 'private component', such as free speech and freedom of information, find little or no protection in the right to (informational) privacy and are possibly neglected when it comes to issues of information and communication technology and liberty.

Moreover, since privacy is generally regarded as an individual right, individuals can willingly and unwillingly release (sensitive) personal information into the public domain themselves. As I will describe more in depth in section 6.4, the vagueness and high levels of abstraction associated with the right to privacy coupled with the unclear distinction between 'the public' and 'the private', contribute to a situation where individuals unwittingly release personal information leading to a *de facto* erosion of liberty.

6.3.2 Privacy and positive liberty

The concept of positive liberty is all about making rational and informed choices about what is right in life. As we have seen in section 6.1, we can only make free and rational choices if we are granted some measure of privacy. The Panopticon shows us that a man who has absolutely no privacy cannot make any choices for himself and is thus enslaved. It may be concluded that privacy surely plays an important role in safeguarding the concept of positive liberty. The Panopticon is a power structure that creates power asymmetries through total surveillance and separation. If surveillance is made less effective

by granting the observed a measure of privacy, the balance of power will shift somewhat towards the observed. As such, privacy protects positive liberty.

The way the privacy can protect us from manipulation and coercion in the 'Superpanopticon' is less straightforward than it is in Bentham's model prison. As I shall describe in section 6.4, the relationship between electronic surveillance, (informational) privacy, and liberty in the information society is far less clear than the relationship between surveillance and privacy in Bentham's Panopticon.

When we take the Christman's (1991) interpretation of the concept of positive liberty, that is freedom from coercion and manipulation, we can establish that positive liberty is more concerned with the second line of privacy theory described in section 5.4, which conceptualises informational privacy as a means to guarantee self-determination and autonomy. The idea is that by setting rules for the use of personal data we can avoid the negative effects of extensive surveillance, mostly notably those caused by the Panopticon and the unseen Panopticon. But while (informational) privacy plays an important role in safeguarding positive liberty, other human rights such as the right to equality, freedom of speech, and freedom of association, also play an important role in the freedom of the individual and that of society as a whole. I shall elaborate further on this issue in the next section and in chapters 7 through 9.

6.4 Difficulties with the right to privacy in the information society

So far the main argument of this chapter has been that it is unlikely that the right to privacy, particularly in its current conceptualisation, can guarantee the complete protection of both the negative and positive concepts of liberty. In this section I shall explain why I feel the right to privacy as it is currently being conceptualised in both the law and the political discourse is inadequate for the complete protection of privacy and individual liberty. I contribute this in no small measure to the rise of new surveillance technologies such as software agents. Furthermore, I shall argue that a pre-occupation with the current approach towards (informational) privacy is counterproductive and could even be detrimental to the protection of (individual) liberty in the information society. The reason for the possible counter-productivity of the right to privacy lies in several separate but interrelated factors, as I shall explain in this section.

I feel that the difficulties with the interpretation of the right to privacy in the information society are of a fundamental nature. As such the problem with the current conceptualisation of privacy is apparent in both the role of privacy in relationships between private entities (such as individuals and businesses) and in the relationship between public bodies and citizens. Therefore, I shall discuss the difficulties with regard to privacy for both the public and the private sector even though the focus of this thesis is on state surveillance.

6.4.1 Vagueness and context

In my opinion the main problem with the right to privacy in the information society is the high level of abstraction involved in fathoming its meaning and importance. The inherent vagueness of privacy, the different conceptions of the right, and the dimensions to which these conceptions apply, contribute to the fact that many people are unable to appreciate the importance of the right to privacy. The preoccupation with the right to privacy could even distract us from the real issue at hand when it comes to surveillance and control: the protection of (individual) liberty.

The fact that more dimensions and conceptions of privacy are conceived and incorporated into the right to privacy leads to what Blok (2002, p. 319) calls an 'inflation' of the private sphere. The inherent vagueness of the right to privacy is amplified by the inclusion of personal data into the private sphere, resulting in a right with such a vague subject matter, that its precise scope and content are unclear to almost everybody in society.

Because of the high level of abstraction, the importance of the right to privacy is oftentimes underestimated. Many people feel they have nothing to hide and are willing to trade an illusive, intangible concept like privacy for clear benefits such as convenience, monetary gain, or increased security.[5] Oftentimes, the importance of the right to privacy is only realised when a damaging infringement of privacy becomes apparent. I believe the reason that most people disregard the importance of privacy lays mainly in the fact that though the right to privacy has changed, it is still associated primarily with the *inaccessibility* of a *personal* sphere, the traditional way of understanding privacy that Solove (2004b) has labelled the secrecy paradigm. In this view privacy is invaded when surveillance uncovers hidden facts. Most people want to hide the intimate parts of their life (for instance, sexuality) from outside scrutiny, but most likely not the fact they regularly buy a certain type of mineral water or visit a particular location. If behaviour is not 'private' enough to hide, we are more prone to exchanging our right to privacy for other privileges, such as customer benefits or a real or perceived increase in security. In particular, when it comes to serious crime and terrorism people are more prone to give up privacy (Koops and Vedder 2001).

Furthermore, the willingness of individuals to disclose personal information is highly dependent on the context. Personal information that people surrender willingly to a certain party in one context, may be kept a secret in another context. But as Solove (2004b) points out, the secrecy paradigm is unresponsive to life in the information society, where most personal information exists in the record systems of hundreds of entities that make up the surveillant assemblage. While the disclosure of individual pieces of information in the

5 See for instance: The European Union Research Group, *Data Protection,* Special Eurobarometer no. 196, December 2003, p. 60.

surveillant assemblage might seem trivial when viewed in isolation, a combination of individual pieces of information can lead to the creation of a fairly comprehensive digital dossier. The dangers of information power do not lie primarily in surrendering individual pieces of (personal) data to different parties, but rather in linking different pieces of data from varying sources within the surveillant assemblage. However, when and how data is being linked is unclear and as a result most people in society are unaware of potentially damaging infringements on privacy and liberty. They associate the surrendering of personal data mainly with liberal surveillance and often fail to make a connection with the possibilities of disciplinary surveillance.

6.4.2 Public versus private

Technology has a profound impact on the way we structure society. The impact that information and communication technology has on our society is reflected in our ideas about privacy and liberty. Warren and Brandeis, for instance, wrote their seminal article at the end of the 19th century when the development of mass media and photography took place. Other important instances that shaped the face of privacy were the development of wiretaps to eavesdrop on phone conversations, the use of computers and databases, and the use of closed circuit television cameras.

By definition the right to privacy is based on a distinction between the public and the private. What belongs to the private sphere is eligible for protection by the right to privacy. But we can establish that the distinction between a public sphere and a private sphere becomes increasingly hard to draw in the information society as a result of advancing technology and accompanying societal changes. It follows that the area that is to remain free from outside interference becomes equally hard, if not impossible to distinguish. In the 18th, 19th and the better part of the 20th century, physical borders such as the walls of our home provided a clear boundary between the public and the private. However the advent of information and communication technology is continuously blurring the border, making decisions about what is private and what is public progressively more arbitrary.

The current legal framework for the protection of privacy, which has its basis in the secrecy paradigm and makes a clear distinction between the public and the private, will face increasing difficulties in the future when it comes to protecting liberty. Solove (2001) notes that since privacy law has developed mainly with the secrecy paradigm in mind (especially in the United States), information that is not considered secret or part of the personal sphere is often excluded from the constitutional protection of privacy.

An example to illustrate this point is the automatic surveillance that was conducted during the 2001 Superbowl. CCTV cameras with facial-recognition capabilities scanned all attendees at a Superbowl Match in Tampa in an effort

to find terrorist suspects. The potential for control embodied in such a technology is evident, yet individual liberty was not protected by the right to privacy. The reason was that in the case of *United States v. Dionisio,* the Supreme Court held that the physical characteristics of a person's voice, handwriting, or facial characteristics, being continuously exposed to the public view, are not within the protection of the Fourth Amendment.[6] Therefore, the use of facial-recognition technology falls outside the scope of the protection provided by the right to privacy in the United States.

Here we see that technology has created a new situation that is difficult to address using classic ideas about privacy. As the example shows, it is possible to identify an individual uniquely using artificial-intelligence technology and closed-circuit television, something that poses a potential threat to individual liberty. The question is whether in order to protect individual liberty we must reinterpret the right to privacy and extend it into the public sphere (which would amount to a blanket right to privacy). If not, do we then have to find other mechanisms to ensure the constitutional protection of liberty?

The European Court of Human Rights took a different approach to this problem. In the case of *Halford v. the United Kingdom* the Court acknowledged that while a person might have a subjective expectation of privacy in the public space, it is not necessarily the conclusive factor on determining whether the right to privacy can be invoked:[7]

> "There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character."

But the Court also held that:

> "Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method."

---

6 *United States v. Dionisio,* 410 U.S. 1, 41 LW 4180 (1973).

7 Case of *P.G. and J.H. v. the United Kingdom,* application no. 44787/98, 25 September 2001.

So, we may conclude that in Europe the right to privacy can be extended to the public sphere when data is being recorded, which brings us to the reasonable expectation of privacy.

6.4.3 The reasonable expectation of privacy

When the line between the public and the private becomes harder to draw, it also becomes more difficult to establish what a 'reasonable expectation of privacy' is. Both the United States Supreme Court and the European Court of Human Rights use the reasonable expectation of privacy criterion in judging violations of article 8 ECHR. The use of the 'reasonable expectation of privacy' criterion has been widely criticised as useless, simply because reasonable expectations of privacy in a situation can disappear as soon as someone starts routinely invading privacy in that situation (Agre 2001). Many people already have the idea that due to information and communication technology everything about them is known and thus have no reasonable subjective expectation of privacy.

The reasonable expectation of privacy criterion limits the right to privacy to those instances where an individual indeed has a reasonable expectation of privacy. In other words, the individual must demonstrate the wish that his conduct remains private and society must acknowledge the fact that the individuals conduct is indeed private. The reasonable expectation of privacy thus entails two separate elements: (1) an objective element (how does the individual behave?), and (2) a subjective/normative element (on what can the individual rely upon judging from his behaviour?). The answers to these separate questions determine whether there is a reasonable expectation of privacy. An indication that an individual may have a reasonable expectation of privacy can be that his behaviour takes place in an area that is considered 'private', examples being a house, car, or dressing room. But as our environment is becoming increasingly networked and transparent, those places that are truly private begin to recede. As a result the area that is considered to be private by both the individual and society is shrinking. The result is not only less privacy, but also less liberty.

Moreover, a judge (at least in the United States) could rule that an individual has no reasonable expectation of privacy with regard to personal data willingly surrendered to a third party or made publicly available by the individual. So, the protection provided by the reasonable expectation of privacy criterion is fairly limited. Moreover, as 'privacy sensitive' technologies continue to develop, how will the reasonable expectation of privacy criterion hold up in the future? For instance: does a person have a reasonable expectation of privacy with regard to the files stored on a computer that is connected to the internet? Or does a person have a reasonable expectation of privacy with regard to the RFID-tags in his house that possibly transmit personal data? These

questions will become increasingly important over the next few years as we move to an increasingly networked environment.

6.4.4 Individual right

Privacy is generally regarded as an individual right. When it comes to the protection of liberty this poses several interrelated problems that I shall summarise in this subsection. I discuss responsibility, control of personal data, power structures, and the individual versus society.

Responsibility
Most legal systems place the responsibility for the protection of privacy -for the greater part- in the hands of the individual.[8] It is up to the individual to make the choice when to disclose what to whom. In particular, in data protection law, which is strongly influenced by the concept of informational privacy as conceived by Westin, the individual's own responsibility is crucial.

As we have seen in the previous sections, individuals must often base decisions on the protection of their privacy on abstract, vague, and incomplete information. Apart from this, the fact that each individual bears responsibility for his personal data, can lead to a situation where the right to privacy is turned into a 'commodity' that can be traded for other benefits. Prime examples of this are customer-loyalty programmes. Consumers give information about their shopping behaviour in exchange for extra benefits, such as lower prices, free gifts or better service. While tailor-made service is not necessarily a problem and offers clear benefits to consumers, a situation could develop where social and economic autonomy is only available to those who can afford to retain their privacy.

Data protection law does not mitigate this possible negative effect of the right to privacy as individual right. The European Data Protection Directive (95/46/EC), for instance, allows for the processing of personal data if the data subject consents to the processing of his personal data. In my opinion this provision is the Achilles heel of the Data Protection Directive as certain categories of consumers that are less affluent could to some extent be 'coerced' to divulge their personal information in exchange for cheaper goods and services. Though in theory a person must always have a free choice, practice shows that a truly free choice is seldom available, as a more 'privacy friendly' alternative is almost always more expensive or less convenient.

Information relinquished to private parties could also be used for disciplinary surveillance by the government. The most obvious way in which the government can use private-sector databases is for the purpose of a criminal

8 This is somewhat different for criminal law where privacy acts more as a restraint on the conduct of law enforcement.

investigation. A second way in which the government can use private-sector databases is for monitoring compliance with special laws. For instance, in his book *Overseers of the Poor* Gilliom (2001) gives striking examples of welfare surveillance. Gilliom describes how private-sector databases are used to check whether welfare recipients act in accordance with information given by them to the welfare authorities. His study shows that the use of private-sector databases contributes to a sense of helplessness and panoptic feelings among the welfare recipients that are subjected to the surveillance.

Control of personal data

The concepts of informational privacy and informational self-determination are difficult to implement when individuals are unaware of the things being done with their personal data. The concept of informational self-determination is only feasible when full knowledge about the amount and types of information being gathered and processed is available to individuals. Without this knowledge, informational self-determination and the accompanying right to informational privacy and are no more than paper tigers.

As surveillance technologies gradually become more pervasive, ubiquitous, and comprehensively networked, knowledge about what is being done with personal data will be increasingly hard to come by. For instance, RFID enables data collectors to collect (personal) data surreptitiously from data subjects carrying RFID-tags, software agents can collect personal data of data subjects from a variety of sources, and CCTV cameras can identify and follow data subjects over large distances. Gaining knowledge of how, when, and to what end personal data is being gathered will become an increasingly difficult task for data subjects in the future if tools are not provided that help them with this task.

Power structures

The exercise of power and control is not by definition aimed at an individual. As such the right to privacy is often unresponsive to the power structures created through the use of information. Many forms of control do not need a distinction at the personal level. The panoptic sort, for instance, operates (in part due to incomplete information) on classification and assessment of (consumer) categories. Individuals are assigned to a certain category and treated accordingly based on limited information. The fact that an individual has a certain age, gender, or ethnicity can already be sufficient to assign the individual to a certain category. Furthermore, additional information on this category need not be supplied by the individual if others belonging to the same category have already done so. This kind of categorisation based on a general profile can influence both the negative and positive liberty of an individual, but it is unclear how the right to privacy can counter the negative effects of this type of information use.

The individual versus society
The final problem with privacy as an individual right is the fact that is often placed against the interests of society as a whole. As such, the right to privacy often loses in the public debate. In my opinion, this problem with the right to privacy is so profound, that I shall devote a seperate section to it, *viz.* on bad publicity.

6.4.5 Bad publicity

The last problem to be addressed is that of the 'bad publicity' surrounding the right to privacy. In an effort to curb rising crime rates and out of fear for international terrorism in the wake of the September 11 attacks, a growing security culture is emerging in many western states, most notably the United States, the United Kingdom, and the Netherlands. In order to prevent terrorist attacks and curb the efforts of organised crime a shift is taking place from reactive investigations (i.e., after the event has taken place) towards more pro-active investigative efforts (Brouwer 2000).

Much trust is placed in surveillance measures, such as cameras, biometrics, and data mining, that must aid in detecting the signs of organised crime or terrorism in an early stage. By establishing a greater degree of control, public administration feels that security can be increased. Since privacy places a limit on the effectiveness of surveillance and thus limits control, the right to privacy has received a great deal of bad publicity.

Privacy is oftentimes portrayed by public administration as a safe haven for criminals and terrorists in which to plan criminal activities without having to fear the prying eyes of law enforcement. The chief of police of Amsterdam for instance has called privacy 'a hiding place of evil'.[9] In its annual report for 2003 the Dutch Data Protection Authority (2004, p. 3) notes:

> "In the public debate the call for more control measures predominates, while the protection of the personal sphere is mainly seen as an obstacle. The Dutch Data Protection Authority is concerned about the erosion of the awareness that personal data may only be processed when it is truly necessary. Restraint in the collection, use, and storage of personal data remains essential."[10]

Shortly after the terrorist bombings in London of July 2005, a study conducted in the Netherlands showed that more than 60 per cent of the Dutch people

9 "Recht op privacy is schuilplaats voor het kwaad" (NRC, 20.11.2003).

10 "In het publieke debat klinkt vooral de roep om meer controlemaatregelen waarbij bescherming van de persoonlijke levenssfeer als obstakel wordt gezien. Het CBP is bezorgd over de erosie in dat publieke debat van het besef dat persoonsgegevens alleen verwerkt mogen worden voor zover dat werkelijk noodzakelijk is. Maatvoering bij het verzamelen, gebruiken en bewaren van persoonsgegevens blijft geboden."

were willing to trade privacy and liberty for enhanced security.[11,12] As fear and feelings of unsafety continue to grow due to the threat of international terrorism, it is likely that privacy will be sacrificied to an increasing extent in favour of a (perceived) feeling of security.

6.5 Provisional conclusion

Privacy and individual liberty are closely related since privacy is a prerequisite for personal autonomy. The conception of privacy as limit to power forms a major part of contemporary thinking about privacy and liberty, in particular when it comes to the relation between the state and its subjects. But due to changes in our society, many of which can be traced back to technological developments, the conception of privacy as a limit to power is facing increasing difficulties.

The right to (informational) privacy plays an important role in limiting the amount of interference into an individual's life and as such is part of the tradition of negative liberty. Surveillance is a specific type of interference aimed at increasing the amount of control that can be exercised over someone or something. Privacy limits the effectiveness of surveillance by shielding the individual's private sphere, in so doing limiting the amount of personal information that can be obtained by a third party. Here we may conclude that the conception of privacy as limit to power has become the predominant function of the right to privacy in the information society and that this function is above all aimed at securing the individual's right to personal liberty. When it comes to the issue of personal data protection, the tendency to invoke the right to privacy in order to curb information power is even stronger.

Whether it is wise to employ the right to privacy as the primary defence against attacks on individual liberty remains subject of discussion, but what is important to acknowledge is the fact that the preoccupation with the right to privacy has led to a situation where privacy and liberty have become values without a clear distinction, leading to much confusion about the scope, application, and importance of the right to privacy. Even in its current incarnation, the right to privacy relies on a distinction between the public and the private that is becoming increasingly hard to make in the information society. The distinction between the public and private, crucial to the concept of privacy, also means that certain aspects of positive and negative liberty that do not have a 'private component' are neglected. Moreover, due to the high levels

11 TNS NIPO, July 8, 2005

12 Ironically, London is the mostly closely surveilled city in the world. Still, these surveillance measures could not prevent the terrorists from targeting the heart of London. It must be said, however, that the available surveillance data did expedite the search for the terrorists.

of abstraction involved in grasping the meaning of privacy, the importance of privacy and personal data protection are oftentimes underestimated.

My idea is that one of the problems facing privacy is that it is still primarily associated with hiding and concealment (i.e., the secrecy paradigm). This general idea leads to a twofold problem. The first part of the problem is that people feel they have 'nothing to hide' and are willing to share a large amount of information that could potentially be used for the purpose of (social) control. Furthermore, the idea of concealment is giving way to a realisation that information is available to anyone. Amongst other things, such an idea puts strain on the reasonable expectation of privacy criterion which is still of great importance when it comes to judging infringements on the constitutional right to privacy. The second part of the problem involves the public opinion towards the right to privacy. In the public debate (in particular when it comes to terrorism) privacy is not seen as a human right and an instrument in maintaining the balance of power between the government and individuals, but rather as a 'hiding place of evil'. Much of this problem can be associated with the fact that privacy is an individual right, which must be balanced against the interests of society as a whole.

So we see that technological developments (of which agent-enabled surveillance is particularly relevant) as well as public opinion put pressure on the right to privacy and its role in guaranteeing liberty. In my opinion the right to privacy is therefore in the future to a large extent an inadequate principal barrier against the possible abuse of power. It seems that (informational) privacy is not the only approach we must take to ensure liberty and it might even be detrimental if we continue to do so. It can be imagined that different mechanisms for the protection of liberty will be needed in addition to the right to privacy, or that the current legal framework for the protection of privacy needs revision. What these mechanisms or changes might be will be discussed in the following chapters.

7 Privacy and liberty in the light of software agents

As you can see we have had our eye on you
for quite some time now, mister Anderson
Agent Smith, the Matrix

In chapter 4 I concluded that the main effects of software agents on surveillance practice are (1) more efficient mediation and query brokering, (2) augmentation of human surveillance operators, and possibly in some areas (3) the replacement of human operators. In this chapter I shall describe how these effects on surveillance practice might in turn influence privacy and liberty. Based on the conclusions of this chapter we can ascertain whether the legal framework for the protection of privacy and liberty is adequate when it comes to agent-enabled surveillance.

I believe that surveillance practice will become more efficient, more user friendly, and more complete through the use of agent technology. I also believe that most applications of agent technology for surveillance purposes will not fundamentally alter the nature of surveillance. In a sense, software agents 'add' to an already existing situation, namely, the rapid expansion of surveillance as a result of the use of information and communication technologies. So for the most part the effects of agent technology on surveillance (and thus on privacy and liberty) are of a quantitative nature, in other words, they merely change the scale on which surveillance is conducted. But apart from the quantitative effects of agent technology on surveillance (and thus on privacy and liberty) I believe certain characteristics of software agents may influence surveillance practice in a more fundamental way. These characteristics (autonomy for instance) set software agents apart from other information and communication technologies that can be used for surveillance purposes. It is my belief that these characteristics and their effects on surveillance will lead to a qualitative change in the application of surveillance technology. If agent-enabled surveillance will -at least in part- differ fundamentally from current surveillance practice, it is possible that the current legal framework is ill-equipped to deal with the effects of agent-enabled surveillance since it was put in place before the advent of agent-enabled surveillance. Therefore, I feel that a differentiation between the *quantitative effects* of agent technology on surveillance (and thus in turn on privacy and liberty), and *qualitative effects* of software agents on surveillance must be made.

I shall start by discussing the quantitative effects of agent-enabled surveillance on privacy and liberty in section 7.1. In section 7.2 I shall describe some (possible) qualitative effects of agent technology and their relation to privacy and individual liberty. In section 7.3 I shall make some general remarks about the future of privacy and liberty in the light of agent technology based on the conclusions of sections 7.1 and 7.2. After we have established the quantitative effects of agent technology on privacy and liberty and discussed the qualitative effects of agent technology. In section 7.4 I shall provide some provisional conclusions in the form of some expectations about the future of privacy in the light of agent technology.

7.1 Quantitative effects of agent technology

Most, if not all surveillance technologies have an impact on privacy and liberty to a certain degree, some by themselves, some in combination with others. This can also be said of agent technology. Based on the conclusions of the previous chapters, particularly chapter 4, I believe that agent-enabled surveillance will have a significant impact on privacy and liberty in the (near) future.

Moreover, I believe that the impact of agent-enabled surveillance on privacy and liberty will be mainly of a quantitative nature. That is to say, the use of agent technology for surveillance will have a measurable effect on privacy and liberty, but the application of agent technology as such does not form a break with past surveillance practices and the possible threats they pose. Arguably, this means that up to a certain level the existing legal framework is adequately suited to deal with the quantitative effects of agent technology.

Below I shall describe five quantitative effects that agent technology will have on surveillance and thus on privacy and individual liberty. They are: (1) more efficient data monitoring and data gathering (subsection 7.1.1), (2) more effective data exchange and data mining (subsection 7.1.2), system integration (subsection 7.1.3), empowering surveillance operators (subsection 7.1.4), and replacing surveillance operators (subsection 7.1.5). These five quantitative effects will be handled as follows. In chapter 7 they will be discussed, in chapter 8 they will be reviewed according to the current legal framework, and in chapter 9 recommendations will be given for the enhancement of the legal framework.

7.1.1 More efficient data monitoring and data gathering

A first quantitative effect of agent technology is more efficient data monitoring and data gathering. We have seen that information overload is one of the

primary reasons to use agent technology. By using software agents, surveillance operators and law enforcement officers can overcome the information overload.

Tools that help overcome the information overload are particularly useful on the internet. The internet houses an enormous amount of information. Unfortunately most of this information is in unstructured form (i.e., natural language). This means that it is difficult to extract useful information from all the available data in an efficient matter. By using agent technology law enforcement agencies can search larger parts of the internet for information that is relevant to an investigation. In addition, agents that are able to interpret natural language can make better sense of unstructured data on the internet. When the semantic web becomes a reality, software agents will become even more effective at monitoring and gathering data.

Furthermore, since software agents are particularly well suited for unobtrusive monitoring, they can be used to monitor data sources continuously online. Obviously, this development will make surveillance and monitoring far more effective, and threats to privacy and liberty more likely.

7.1.2 More effective data exchange and data mining

A second quantitative effect of agent technology is its contribution to more effective data mining. In particular in the area of (distributed) data mining, agent technology can have a profound impact on the efficiency with which data is integrated. As we have seen in chapter 4 software agents can be used to integrate heterogeneous, disparate, and geographically distributed databases into a single 'virtual database', making data mining (and thus surveillance and control) far more effective.

We have established that technical barriers to accessing and processing personal data lead to inefficiencies that act as *de facto* safeguards for privacy and liberty. The protection of privacy and liberty in the information society is for a large part dependent on these inefficiencies. Where there are no technical barriers to accessing and processing personal data, the legal framework puts in place artificial inefficiencies in the form of regulation that forbids aggregation and integration of databases. So, on the one hand there is a need to connect the dots, while on the other hands there is the notion of a free society that seeks to keep the power to connect the dots away from any one actor, particularly the central government (Taipale 2003, p. 58).

We have established in chapter 3 that we can distinguish between two approaches in data mining, *viz.* subject-based inquiries and pattern-based inquiries. Both influence privacy in different ways, so I shall describe their effects separately.

Subject-based inquiries and privacy

Agent technology enables surveillance operators to query many databases simultaneously in search of information regarding a specified individual. Furthermore, software agents can also search the internet for information regarding a specified data subject (the idea of dataveillance). So, we may conclude that through agent technology subject-based inquiries will become more efficient, effective, and complete.

Extensive aggregation and integration of data can ultimately lead to what Taipale (2003, p. 58) calls 'the demise of practical obscurity', a situation where an individual is unable to hide himself from outside scrutiny. Such a situation is detrimental to an individual's privacy and liberty. As described throughout this thesis substantial digital dossiers regarding individuals can be used to exercise (social) control. The more efficient the aggregation and integration of personal data becomes (for instance through agent technology), the more profound its effects on privacy and liberty will be.

Apart from the exercise of direct control through knowledge gained from a subject-based inquiry, there are also panoptic effects associated with data aggregation and integration. Extensive aggregation and integration of personal data can have a chilling effect on individual behaviour (Minow *et al.* 2004, p. 35). As a result of extensive government oversight or the possibility thereof, individuals might refrain from certain social or commercial activities, mask their behaviour, or reduce their participation in society out of fear of judgement. The risk is not only that social or commercial activities are chilled, but also that rights such as the freedom of expression, protest, association, and political participation are affected as well (Minow *et al.* 2004, p. 35). What must be noted is that for panoptic effects to occur it is not actually necessary for agent technology to be as effective as suggested. The mere idea that software agents can gather information is enough to cause panoptic effects. In other words, knowledge is power, but potential knowledge can equally present power (Minow *et al.* 2004, p. 35).

Pattern-based inquiries and privacy

Software agents can also facilitate pattern-based inquiries through distributed data mining. The problem with pattern-based inquiries from the perspective of privacy and liberty is that the data analysis is not based on an individualised suspicion. In other words, everyone is a potential suspect. If your behaviour matches certain criteria, you automatically become a suspect. This kind of proactive searching for criminal behaviour that has yet to take place is reminiscent of Dick's novel *The Minority Report*, in which mutated humans called pre-cogs are able to predict future crimes (Dick 1956, p. 71-101).[1] In the book the pre-

1 In 2002 *The Minority Report* became a major motion picture starring Tom Cruise. Though the plot of the movie differs somewhat from the book, the central theme of surveillance and control remains.

cogs are able to witness a murder before it actually takes place, thus making it possible to apprehend the potential killer in advance. The obvious effect this has is that premeditated killings become a thing of the past. The potential panoptic power that flows from this 'precognition' is evident. While these effects might be desirable in the case of murder or terrorism, there are many situations where such power is less likely to be desirable. Of course, pattern-based inquiries do not have the same level of precision and accuracy as the technology described in *The Minority Report*, but the idea is more or less the same.

The idea that the government is able to match certain behaviour automatically to a 'suspicious pattern' can lead an individual to adopt a behavioural pattern that is more consistent with the perceived social norm. By defining which behavioural patterns are considered deviant, the government can effectively regulate individual behaviour. For instance, it is possible that people will alter their behaviour to avoid being considered a potential suspect by refraining from conducting activities that might be categorised as 'high risk' activities. So, when pattern-based inquiries are used for the purpose of regulating behaviour positive liberty is at stake. The use of pattern-based inquiries might be justifiable for the prevention of terrorism and organised crime if adequate safeguards are in place, but there is always the risk of function creep.[2] Moreover, as the behavioural patterns of political and social minorities are more likely to be labelled as suspicious or deviant, there is also the risk of discrimination and social inequality.

7.1.3 System integration

A third quantitative effect of agent technology is its contribution to system integration. In section 3.2 I have described the rhizomatic expansion of surveillance throughout society. Our growing reliance on surveillance for security, efficiency, and convenience has prompted the installation of many different surveillance systems and infrastructures, both in the public and in the private sector. Though surveillance systems of both a liberal and a disciplinary nature are being deployed by a variety of actors without a centralised, hierarchical structure, there is a strong desire (especially on the part of the government) to bring these systems together and integrate them into a larger whole. In general, surveillance systems are built with a specific purpose and surveillance

2 An example of function creep can be seen in the MATRIX (Multi State Anti-Terrorism Information eXchange) programme. The MATRIX was a tool for large-scale data-exchange commissioned by several states in the United States in response to the September 11 terrorist attacks. It combined information from a multitude of public sector and private-sector databases to aid law enforcement officers in the identification of terrorists. However, according to figures issued by the programme itself, just 2.6 per cent of all the queries to the system were actually related to terrorism (Seifert 2006).

domain in mind. Typically, these systems employ only a single type of surveillance technology (for instance, CCTV, RFID, or GPS). Consequently, surveillance systems are not developed with interoperability in mind. However, combining different kinds of surveillance mechanisms and integrating different surveillance systems into a larger whole can greatly enhance the overall effectiveness of surveillance, in particular in the area of (automated) monitoring. Information and communication technology plays an important part in this development, as it allows for the rapid expansion and integration of surveillance (Lyon 2003b, p. 94).

Among the technologies for integrating surveillance mechanisms and systems, software agents feature prominently. As I concluded in section 4.5, software agents provide mediation services and query brokering to surveillance operators by enabling logical and semantic interoperability of (previously) discrete surveillance mechanisms and systems. The most striking examples of integrated surveillance systems are the sensor networks and (collaborative) decision-support systems described in chapter 4. These sophisticated surveillance networks provide a glimpse into a possible future for surveillance and control. Furthermore, they illustrate how powerful 'next generation' surveillance might be and how it will influence privacy and (individual) liberty.

The lack of interoperability between different surveillance mechanisms and systems acts as a *de facto* safeguard against excessive surveillance powers. However, as we can judge from the development of distributed data-mining systems, collaborative decision-support systems, and C4ISR systems, ongoing system integration made possible by software agents is rapidly removing technological barriers to system integration. By combining different types of surveillance systems into a larger whole a more complete surveillance infrastructure can be created. Naturally, a more comprehensive surveillance infrastructure has adverse effects on privacy and liberty. In a sense, agent technology 'multiplies' the effectiveness of (previously) discrete surveillance systems. In this way, system integration will enhance the possibilities for the exercise of control, threatening privacy and liberty. Moreover, system integration will contribute to the panoptic feelings felt by those being watched.

7.1.4 Empowering surveillance operators

A fourth quantitative effect of agent technology is the way in which it can empower surveillance operators. The improvements in logic and semantic interoperability that agent technology provides, makes surveillance operators more effective in general. But apart from improving logic and semantic interoperability, software agents can also empower surveillance operators by making their job easier. Software agents can make surveillance operators more effective by acting as 'personal assistants' (i.e., the COPLINK Active Agent) to

surveillance operators or by providing decision support (i.e., COORDINATORS and COMBINED systems). This means that surveillance is enhanced, which in turn may pose an additional threat to privacy and liberty.

The obvious threat to privacy and liberty is the more effective exercise of control as a result of enhanced surveillance. However, it is more difficult to establish if panoptic effects can be associated with the empowerment of surveillance operators. Panoptic effects only occur when people are aware of the fact that surveillance is being conducted. I feel it is unlikely that people will realise how software agents will make surveillance operators more effective. If this holds true, panoptic effects will be limited. However, when people do realise how software agents might improve the capabilities of surveillance operators, panoptic effects will become stronger.

7.1.5 Replacing surveillance operators

A fifth quantitative effect of agent technology is that in some instances it can replace surveillance operators. Software agents could thus eventually, at least in part, remove the need for human operators. Examples of monitoring tasks that can be performed by software agents are the autonomous operation of CCTV cameras and surveillance of the internet. In view of the fact that software agents are less expensive in operation than their human counterparts, it is likely that they will be employed more often. This will make surveillance more comprehensive both in scope and duration, particularly in the area of (automated) monitoring. The fact that surveillance will become more comprehensive will no doubt have an adverse effect on privacy and liberty and further strengthen the Panopticon.

As of now it is unclear what the impact of automated surveillance will be on privacy and liberty. At this stage there are not that many applications of agent technology whereby human operators are replaced. The XENON application is one of the first working examples of agent technology taking over the tasks of human operators. In my opinion the impact of automated surveillance will be profound, but in this stage of the development it is too early to draw any definitive conclusions.

7.1.6 Conclusions on quantitative effects

I described how agent technology can contribute to the exercise of surveillance and control. It may be concluded that the quantitative effects of agent technology on surveillance will result in more efficient, more effective, and more comprehensive surveillance. However, this development may also have adverse effects on privacy and liberty when adequate safeguards are not put in place.

The use of agent technology for surveillance purposes is part of a broader development towards the more effective and efficient exercise of surveillance by means of information and communication technology. The quantitative effects of agent technology must not be viewed in isolation, but rather in the light of this broader development. Yet, the quantitative effects of agent technology could accelerate the development of a more complete surveillance infrastructure. Therefore, we may conclude that it is likely that agent technology will further broaden the 'information divide' that exists as a result of surveillance. I use the term 'information divide' to describe the discrepancy in information available to the observers and the observed. Those who have access to advanced agent technology will have better access to information and will more easily gain knowledge, upsetting the balance of power. Agent technology could have a 'multiplier' effect on the existing information divide since software agents are so effective in finding information and making sense thereof for human operators.

7.2 Qualitative effects of agent technology

Owing to some of their unique characteristics, software agents might influence the surveillance practice in such a way that their application will yield effects currently unimagined. Among the unique characteristics likely to influence surveillance in the future are: (1) autonomy, (2) emergent behaviour, (3) adaptive capabilities, and (4) mobility. The application of software agents and multi-agent systems that display these characteristics might lead to situations that raise questions with regard to the legal status of their application. Since these specific characteristics cannot be found in other surveillance technologies it could well be that the existing legal framework is not adequately equipped to deal with the effects of these unique characteristics. Therefore, I shall call the effects that flow forth from these four specific characteristics 'qualitative effects' in order to distinguish them from the quantitative effects of agent technology. In this section I shall identify five qualitative effects and describe how they might influence privacy and liberty. Analogously to the quantitative effects I shall describe the five effects in chapter 7, review them according to the current legal framework in chapter 8, and provide relevant enhancements and recommendations for an improved legal framework in chapter 9.

7.2.1 Competence and authority

The first qualitative effect of agent technology relates to competency and authority. What distinguishes software agents first and foremost from other surveillance technologies is their ability to function autonomously. As discussed in subsection 2.10.1, agent technology may have both the technical capacity

as well as the legal authority to function autonomously in a given environment. With the 'classic' surveillance applications direct supervision and control by a human operator is always necessary. The ability to function autonomously contributes much to the quantitative effects of agent technology on surveillance. Software agents that display a high level of autonomy will enhance the overall effectiveness of surveillance and make surveillance more complete. It is possible that this will have an adverse effect on privacy and individual liberty and contribute to stronger panoptic feelings. Combined with adaptive capability, emergent behaviour, and mobility, software agent autonomy has a qualitative effect in that it causes uncertainty with regard to the legal competence and authority of software agents to undertake surveillance tasks without human supervision.

7.2.2 Emergent behaviour

As described in section 2.7 interaction within complex multi-agent systems can trigger the spontaneous emergence of intelligent behaviour. This is our second qualitative effect. Emergent behaviour is a characteristic of software agent (systems) that leads to complexity and uncertainty. From the perspective of privacy and liberty emergent behaviour in surveillance systems is undesirable. Since emergent behaviour is difficult to predict, if not impossible, it is very difficult to regulate. This means that any threat posed by emergent behaviour to privacy and liberty cannot be mitigated by regulation. It is therefore questionable whether a 'grey area' of emergent behaviour is acceptable when it comes to surveillance and privacy.

7.2.3 Adaptation

More advanced software agents have the ability to adapt themselves to changes in their environment. It can be envisioned that in the future, intelligent agents and agent systems will have the technical capacity to adapt themselves in order to perform their surveillance and control tasks better. Thus, over time software agents will become more proficient at performing their surveillance tasks. This is our third qualitative effect.

A simple (and already technologically feasible) example of adaptive agent technology, is an agent that must acquire new skills (such as rules and ontology's) in order to enter a specific database. By acquiring these new skills software agents adapt themselves in order to perform the tasks they were given. More futuristic scenarios include software agents that learn from their experiences and adapt themselves to changes in their environment. Some types of software agents even have the ability to replicate themselves and delegate tasks to their offspring.

The qualitative effect this may have on surveillance is that a software agent that was designed to perform a specific surveillance task might improve itself in such a way that it surpasses its original design goals. Obviously, this will increase the overall efficieny and effectiveness of surveillance, but it will become less clear if enhanced surveillance capabilities fit within the investigative powers granted to the software agent. While adaptive agents might therefore be a boon to surveillance, they are much less so for privacy and liberty when adequate safeguards are not in place. Adaptive agents thus may raise legal questions with regard to their investigative powers that need to be answered in order to minimise any threats to privacy and liberty.

7.2.4 Transparency and insight

A fourth qualitative effect that software agents may have on surveillance is the result of characteristics such as autonomy, emergent behaviour, and adaptive capabilities. We have already established that software agents can access disparate and distributed data sources more easily than traditional data-mining approaches and that this ability influences surveillance in a quantitative manner. The qualitative effect that can be associated with the integration of databases through agent technology is a potential lack of transparency and insight when it comes to the fusion and integration of different data sources.

As we have established earlier in this thesis, 'connecting the dots' (i.e., linking various data sources) may pose a threat to privacy and liberty. Together with rules regarding the integration of data sources, transparency and insight are necessary to minimise the risk of excessive data integration. In the traditional approach to (distributed) data mining, data sources are designated in advance and the data gathered from these sources is fused and integrated. In this way it is always clear which data sources are linked. But with software agents or multi-agent systems that have a high level of (technical) autonomy and a broad mandate it might be less clear. When a software agent or agent system is capable of accessing a large number of different data sources (internet sites, databases, chatrooms, newsgroups) it will become more difficult to determine what pieces of data are being gathered and integrated. It could well be that while an agent is authorised to access two different databases separately, it is not authorised to fuse and integrate information from these databases. The risk now is that though the agent is not authorised to fuse the data, it will still do so.

A related risk that originates from a lack of insight into agent-enabled fusion and integration of data is unforeseen data integration. It is possible that an agent fuses and integrates information from different data sources in a combination that is unanticipated with the current state of technology. The risk this carries with it is that while there is a possible threat to privacy, there are no legal safeguards in place. For instance, there might be no specific rule

prohibiting the fusion and integration of publicly information available on the internet with information contained in police databases, since with the current state of technology it is impossible to do so effectively. It is this lack of insight into the *modus operandi* of an advanced software agent or agent system that could threaten privacy and individual liberty.

7.2.5 Strength of agent metaphor

When one talks about surveillance and control, the idea of Big Brother is oftentimes invoked. Orwell's (1949) metaphor of a powerful state apparatus continuously watching citizens for signs of dissidence has proven to be immensely powerful. While the Big Brother metaphor is primarily used as a cautionary tale, the power of a metaphor can also have a less beneficial influence. This holds especially true for software agents. Therefore, we call this metaphor our fifth qualitative effect.

When it comes to software agents, we can discern a general tendency to anthropomorphise them. I described a good example of this tendency to anthropomorphise software agents in chapter 1, *viz.* Agent Smith from the movie *the Matrix*. Describing software agents as digital equivalents of human surveillance operators or law enforcement officers could raise the suggestion of a 'virtual army' of powerful software agents continuously patrolling the digital world in search of suspicious conduct. Although no clear evidence to this suggestion exists at this time, the extensive use of agent technology can add to the panoptic effects of surveillance.

7.2.6 Conclusions on qualitative effects

The development of agent technology for surveillance purposes is moving ahead at a steadily increasing pace and it is likely that we will see more advanced applications of agent technology over the coming years. The specific characteristics of these more advanced software agents (most notably autonomy, emergent behaviour, adaptive capabilities, and mobility) will have a qualitative effect on the exercise of surveillance. When software agents are used that display the above mentioned characteristics, their application will differ greatly from the application of 'classic' electronic surveillance technologies. As the current legal framework was not drafted with the use of agent technology in mind, it is possible that the qualitative effects of agent technology are not dealt with under current legislation. Therefore, questions need to be asked regarding the legal framework that governs their application. These questions have to do with the legal status of software agents, their authority to conduct surveillance, uncertainty with regard to (emergent) agent behaviour, and their ability to adapt. Dubiety about these specific legal aspects of agent-

enabled surveillance can have a negative effect on privacy and liberty. Thus, it is necessary to establish whether the current legal framework is adequately suited to deal with these qualitative effects.

7.3 THE FUTURE DEVELOPMENT OF AGENT-ENABLED SURVEILLANCE

Though currently the use of agent technology for surveillance tasks is not yet widespread, it is to be expected that the use of agent technology for surveillance purposes will increase over the coming years. So, while the impact of agent technology on privacy and individual liberty might currently be limited, the effects will most likely become more apparent over the coming years.

It is my belief that a potential threat to privacy and liberty made by agent technology will be strongest when software agents with high levels of autonomy operate in an open environment. In section 2.8 a possible timeline for the development of agent technology was given based on the *Agentlink Roadmap* (Luck *et al*., 2003). In the ECP.NL report *Juridische Aspecten van Autonome Systemen* (Schermer *et al.*, 2005) a similar timeline was projected against possible levels of agent autonomy and the openness of their environment. Based on the findings in these reports we may establish that agents currently used in an open environment (such as the internet) have (very) limited technical and legal autonomy.[3] Furthermore, the use of agent technology (especially that of advanced autonomous agents) for the short-term future will be limited to closed systems.

When eventually we do move towards the use of software agents in open environments, the impact of agent technology on privacy and individual liberty will increase substantially. As mentioned in chapter 2 the future development of agent technology in juxtaposition with other key technologies such as RFID, sensor networks, IPv6, grid computing, and embedded systems will ultimately bring about the next big ICT paradigm, that of ambient intelligence (Aarts 2002). Ambient intelligence will provide ample opportunity for surveillance, as much of our surroundings will become networked and intelligent. Moreover, our private sphere (for instance, our home and our clothing) will come into contact with the public sphere more often due to networking. In the ambient-intelligence paradigm software agents could play a pivotal role in the future development of surveillance by acting as gatekeepers, personal assistants, and information brokers.

In any case, it is the quantitative effects of agent technology that will become significant first. In a later stage, when the science of artificial intelligence has advanced further and agents and information systems become

3 English: *Legal Aspects of Autonomous Systems*.

interoperable, the qualitative effects of agent technology will emerge. Currently software agents have very little autonomy, adaptive capabilities, and mobility. As such, they pose a relatively small threat from a qualitative point of view.

7.4 PROVISIONAL CONCLUSIONS

In chapter 4 we looked at several applications of agent technology in the area of surveillance. We established that software agents will primarily be used for three purposes, namely mediation services and query brokering, augmentation of human operators, and the replacement of human operators. The main effects the use of agents will have on surveillance (and thus on privacy and liberty) are (1) more effective data mining, (2) system integration, and (3) the further empowerment of surveillance operators. These effects are of a quantitative nature, that is to say, they contribute to the overall effectiveness of surveillance, but do not change the nature of the surveillance practice itself. As such, these effects do not necessarily raise new questions about the regulation of surveillance and the protection of privacy and liberty. However, the quantitative effects of agent technology do add further weight to the discussion about the balance between surveillance, privacy, and liberty. Surveillance in our society is becoming increasingly pervasive, a situation to which agent technology will contribute in no small measure. It may therefore be concluded that we must take care of ensuring that the current legal framework is prepared for the quantitative effects of software agents that are likely to impact surveillance in the near future.

Apart from the quantitative effects of agent technology we have seen that four unique characteristics, *viz.* autonomy, emergent behaviour, adaptive capabilities, and mobility, can also have effects on surveillance that can best be described as being of a qualitative nature. These qualitative effects raise new questions about the legal framework for the regulation of surveillance and the protection of privacy and individual liberty. The questions have to do with the authority of software agents, the complexity and the uncertainty, and the ability of software agents to adapt themselves to changes in their environment. It is important to address these issues, as uncertainty regarding the legal framework will influence privacy and individual liberty in a negative way.

As we move towards the ambient-intelligence paradigm the significance of both quantitative and qualitative effects will increase, it is therefore necessary to examine the legal framework in an early stage. The question I will try to answer in the next chapter is: can the existing legal framework deal with the possible threats made to privacy and liberty by software agent-enabled surveillance?

8 The legal framework reviewed

You have zero privacy anyway, get over it.
Scott McNealy

As stated throughout this thesis, extensive surveillance and control may threaten privacy and liberty. To mitigate the possible negative effects of surveillance, democratic societies put in place legal barriers that regulate the use of surveillance. What rules apply is dependent on the context in which surveillance is practiced. As mentioned earlier in this thesis, I shall focus on the legal framework that applies to the use of surveillance for the purpose of law enforcement.

Since the goal of this chapter is to determine whether the legal framework for the regulation of surveillance is adequate in the light of agent-enabled surveillance, I shall first describe the general functions that a legal system must perform (section 8.1). In section 8.2 I shall: (1) describe the nature of the legal issues associated with the quantitative and qualitative effects of agent technology on surveillance, and (2) differentiate between possible reactions of the legislator. In sections 8.3 and 8.4 I shall elaborate on the legal issues related to quantitative and qualitative effects. In sections 8.5 and 8.6 I shall argue why I feel that the quantitative and qualitative effects of agent technology impact the legal framework to such a degree, that it needs to be amended.

8.1 The functions of the legal framework

Before we can determine whether the legal framework is still adequate in the light of agent-enabled surveillance we must establish the functions of the law. Legal philosophy and legal theory are concerned with answering questions about the origins, goals, and functions of the legal framework. Important contemporary scholars in the area of legal philosophy are Hart, Fuller, Rawls, and Dworkin. At an abstract level they have formulated answers to questions such as: what is law, what is justice, and what constitutes morality? A more practical approach can be found in the work of Franken (1995) and that of Van Hoecke (2002). They both give transparent and comprehensive summaries

as to what the functions of the law are within society.[1] For the purpose of this thesis I will use Van Hoecke' work as it is more recent. In his book *Law as Communication* Van Hoecke (2002) describes two general functions of the law. Van Hoecke distinguishes between the law as a means to order society (see 8.1.1) and the law as a means to facilitate an indiviual's life (see 8.1.2) (Van Hoecke 2002, p. 65). Within these functions Van Hoecke distinguishes several specific sub-functions. The question in this context is whether the current legal framework can still adequately perform these functions when surveillance is influenced by agent technology. The functions of the law as described by van Hoecke will thus serve as the starting points for the evaluation of the legal framework.

8.1.1 Structuring society

One of the primary functions of the law is to structure society and prevent its disintegration. The law performs this function by structuring political power and maintaining social cohesion.

Structuring political power
In democratic societies political power is structured through the application of (constitutional) law. The primary role of constitutional law is to organise political power. It regulates amongst other things, which institutions will exert what political power, who has the right to political participation, and which procedures have to be followed. Moreover, constitutional law determines which basic rights belong to citizens and, therefore, limit the power of state and political bodies (Van Hoecke 2002, p. 63). In this way the law determines how power is distributed in society and what restrictions apply to the exercise of this power.

Keeping social cohesion
The law has a well-defined function when it comes to maintaining social cohesion. Van Hoecke (2002, p. 64) argues that:

> "the law offers a framework within which citizens may reach understanding on norms and values, realise collective goals, bargain between interest positions and

1 I have chosen the work by Van Hoecke (2002) over the works by other prominent legal theorists such as Hart's *The Concept of Law* (1961), Fuller's *The Morality of Law* (1964), Rawls' *A Theory of Justice* (1971), and Dworkin's *Law's Empire* (1986), because Van Hoecke uses a more functional approach to defining the concept of law. In particular his enumeration of various (societal) functions of the law is helpful, since it enables us to determine more easily whether the legal framework can still adequately perform its different functions in the light of agent-enabled surveillance.

solve conflicts. All this plays an important role in bringing about or keeping social cohesion or integration."

But since choices regarding the content and application of the legal framework will directly or indirectly influence the position of different groups within society, social cohesion can be adversely affected by the application of the law, too.

8.1.2 Facilitating an individual's life

Philosophers such as Hobbes, Locke, and Rousseau concluded that the law liberates us from a state of anarchy. However, the law does more than create a reprieve from anarchy, it creates positive conditions for facilitating human interaction, human communication, and the development of the individual (Van Hoecke 2002, p. 66). There are seven ways in which the law can facilitate an individual's life, *viz.*, by (1) bringing about desirable behaviour, (2) creating spheres of autonomy, (3) coordinating human behaviour, (4) facilitating private arrangements (for instance, contract formation), (5) allocating resources, (6) redistributing goods and services, and (7) solving conflicts (Van Hoecke 2002, p. 67). Of these seven functions the first two are of importance to the subject matter of this thesis.

Bringing about desirable behaviour
The law plays an important part in influencing an individual's behaviour. By steering people's behaviour the law significantly improves our social environment (Van Hoecke 2002, p. 68). The most obvious example of how the law can influence society by steering people's behaviour is criminal law. However, while the law is used to steer people's behaviour, it also limits the extent to which institutions may influence individual behaviour. It does so primarily by creating spheres of autonomy.

Creating spheres of autonomy
Modern democratic legal systems establish 'spheres of autonomy', in other words, they grant individuals a certain measure of freedom that they can use as they see it fit (Van Hoecke 2002, p. 67). This freedom guaranteed by the law may be used for a myriad of different purposes that can be either of a private nature (for instance, making contracts) or a public nature (for instance, participation in the public debate). Within the context of this thesis it is noteworthy that the right to privacy is one of the means to create spheres of autonomy.

8.2 Legal issues and legislative reactions

In chapter 7 we have established that agent technology has both quantitative and qualitative effects on surveillance. The quantitative and qualitative effects of agent technology both affect the legal framework, albeit in their own ways. For the sake of clarity I shall deal with the legal issues surrounding both the quantitative and qualitative effects separately, even though at some points it is difficult to make a clear distinction between quantitative and qualitative effects. Below I shall discuss the legal issues resulting from quantitative and qualitative effects (8.2.1) and the possible reactions of the legislator (8.2.2).

8.2.1 Legal issues resulting from quantitative and qualitative effects

As part of a more general system of society, a legal system is a way of organising social, economic, moral, and other patterns of behaviour (Van Hoecke 2002, p. 37). Thus, a legal system cannot exist independent of society. Therefore, any significant changes in the structure of society, for instance, as a result of advances in technology, need to be reflected in the legal framework. The effects of agent technology act as external influences on the legal system and consequently raise legal issues within the legal system. As I shall describe in the following paragraphs the nature of these legal issues differs for the quantitative and qualitative effects of agent technology on surveillance.

The nature of legal issues resulting from quantitative effects
Dealing with the quantitative effects of agent-enabled surveillance in the law is a difficult task. The problem is that the use of agent-enabled surveillance as such does not necessarily form a radical break with past practices, and the impact of agent-enabled surveillance is therefore not immediately apparent. In essence, the use of agent-enabled surveillance adds to an ongoing situation of intensifying surveillance. This situation is characterised by a tension between privacy and liberty on the one hand, and security, efficiency, and convenience on the other hand. The development of agent-enabled surveillance contributes to the move from a situation of limited surveillance towards a situation of 'total' surveillance. As surveillance becomes more intense due to agent technology, the exercise of control will become more effective as well. In my opinion this development is primarily an issue related to the distribution of power within society. So, any legal issues stemming from quantitative effects are primarily concerned with this issue.

The nature of legal issues resulting from qualitative effects
The qualitative effects of agent technology on surveillance are of an entirely new sort, and consequently they raise different legal issues. These issues have to do with the fact that the legal framework was put in place before the advent

of agent technology. The question that must be asked in this respect is whether the structure and content of the legal framework is adequately suited to deal with the specific characteristics of agent technology and their effects on surveillance, privacy, and liberty. If not, changes to the legal framework need to be made in order to adjust to the new reality.

8.2.2 Legislative reactions

In my opinion, the legal issues described in this chapter will ultimately force the legislator to make changes to the legal framework. At the basis of these changes lies a normative decision. When it comes to making changes to the legal framework the legislator must consider the following question: what balance must be struck between surveillance, privacy, and liberty in a democratic society? This underlying question is the same for both the quantitative effects and qualitative effects of agent-enabled surveillance. However, since the nature of the legal issues associated with the quantitative and qualitative effects is different, they will most likely prompt different legislative reactions.

In the case of quantitative effects, it is my belief that the change in the scale of surveillance will ultimately force the legislator to rethink the structure of the legal framework as a whole. As I have described in chapter 6, the right to privacy has some inherent problems that might render it inadequate as a principal barrier against the negative effects of excessive surveillance in the future. If this is the case the legal framework (with its strong focus on the right to privacy) as a whole needs to be reconsidered, since it will proof to be an ineffective mechanism for maintaining privacy and liberty.

In the case of qualitative effects, a complete overhaul of the legal framework might not be necessary. It is my belief that the legislator must evaluate for each of the qualitative effects whether they can be addressed within the structure of the existing legal framework. If this is the case, the legal framework must be amended to accommodate for these effects.

The best way to clarify the difference between these different legislative reactions is to introduce a metaphor. Assume that there is a public beach. During the summer it is prohibited to ride a horse on the beach because the beach is too crowded. However, during the winter the beach is less crowded, and therefore horse riding is allowed. The rationale behind this rule is that riding a horse on a crowded beach poses a threat to public safety, while riding a horse on the beach when there are few people around does not. Such a rule could be formulated as follows:

> "Horseriding on the beach is prohibited between May 1st and October 31st"

Then we assume that instead of a few horses, one thousand horses would ride on the beach at the same time during the winter (we call this situation 1). In

this situation horses would crowd the whole beach and it would be very dangerous for an individual to walk there. We can see that due to a change in scale in one of the factors (i.e., the number of horses) the entire situation has changed. However, from a legal point of view the situation *has not* changed. It is still a beach where horse riding is allowed during the winter. The rule governing horse riding on the beach has not been broken since it does not state anything about the amount of horses that are allowed on the beach. So, while the rule in itself is still correct and applicable, it no longer provides any relevant protection to people on the beach. Consequently, the change in scale triggers a shift in the nature of the situation to which the legal framework has to adjust, most likely through a thorough revision or reinterpretation of the legal framework.

Next we assume someone has invented an incredibly powerful machine that is able to traverse the beach at great speeds (we call this situation 2). It is clear that such a machine poses the same danger as a horse, if not greater. However, it can be argued that since the legal framework does not prohibit the use of such a machine, it is legal according to the rule under investigation to drive it on the beach. In order for the legal framework to adjust to this new situation, changes need to be made to the existing rule.

In situation 1 no new elements are introduced, but we are faced with a change in scale. As a result, the rule under investigation (i.e., the legal framework) can no longer fulfil its intended function. The change in scale has proven that a ban on horse riding during a certain period is no longer an adequate mechanism for ensuring public safety. Therefore, we must reconsider the structure of the rule as a whole and ask ourselves how it must be revised in order to once again fulfil its intended function.

In situation 2, we are also faced with a new situation. However, in this situation the change is of a qualitative nature, since a new element has been introduced (i.e., a fast moving vehicle) that was not considered when the original rule was drafted. In this case it must be decided whether the existing rule covers the new situation. If not, the rule must be changed in order to incorporate the new element. In the latter case it could well be that the issue can be addressed using the structure of the existing rule under investigation, and that a complete overhaul of the legal framework is not necessary.[2] For instance, the phrase 'and driving fast moving vehicles' could be inserted after the word 'horse riding' to accommodate for the new situation. This would

2 It is not my intention to suggest that the legal issues resulting from the qualitative effects of agent technology will have less impact on society than the quantitative effects. Though the qualitative effects of agent-technology may not require a complete overhaul of the legal framework, their effects could be equally -if not more- profound. However, the 'paradigm shift' that could result from quantitative effects of agent technology will sooner force a decision on the legal framework as a whole, while the legal issues related to qualitative effects can most likely be addressed within the existing legal framework.

address the issue raised by the driving of a fast moving vehicle, without the need for a complete overhaul of the existing legal framework.

8.3 Legal issues related to quantitative effects

Below I analyse the legal issues associated with the five quantitative effects of agent-enabled surveillance we identified in chapter 7. I shall examine each of the quantitative effects in the light of the current legal framework for the protection of privacy and liberty. I do so for both the legal system of the Netherlands and that of the United States.

8.3.1 Efficient monitoring and data gathering

For the execution of the normal police task law enforcement agencies may gather information. This task is made easier by agent technology. In the legal framework of the Netherlands and the United States, there are no provisions that explicitly prohibit the use of automated data gathering in the public sphere.

In the Netherlands the Data Protection Act governs the processing of personal data in general. In the context of a criminal investigation both the Police Files Act and the law of criminal procedure apply. However, this does not give us a clear answer to the question whether software agents may conduct automated surveillance of the public sphere. It could be argued that automated surveillance of the public sphere is part of the normal police task and the use of this investigative method is therefore within the boundaries of article 2 of the Police Act of 1993.

In the United States the general rule is that an individual has no reasonable expectation of privacy concerning information that is disclosed to a third party.[3] For instance, information published on the internet is considered part of the public sphere, and as such Fourth Amendment privacy protection does not apply (Solove 2004b, p. 201). This means that personal data that is available on the internet, or data that is gathered in the public sphere, may be monitored and used for law enforcement purposes. The authority to conduct internet surveillance is confirmed in section D of the introduction to the *Attorney General's Guidelines*.

General surveillance of the public sphere could thus be considered part of the normal police task in both the Netherlands and the United States. With the current state of technology, this is not yet a big issue as gathering and processing personal data from the internet, or (re)viewing surveillance tapes

3 See *United States v. Miller*, 25 US 435 (1976), and *Smith v. Maryland*, 442 US 735 (1979).

manually, is still a daunting task. So, currently we have no legal issues to bring up. However, software agents will certainly change this situation.

8.3.2 Effective data exchange and data mining

Since more effective data mining and data exchange is one of the most significant quantitative effects of agent technology, it is important to determine what its effect is on the legal framework that governs (agent-enabled) data mining. An answer to this question is largely dependent on the phase of the investigation. In particular in the earlier stages of an investigation (before an actual criminal investigation has started) data mining can yield valuable, previously unknown information. The question is whether the legal framework covers the increased effectiveness of policing resulting from more effective data mining.

For the execution of the normal police task automated information gathering, data exchange, and to some extent data mining, may be employed by law enforcement, both in the Netherlands and the United States. There are however certain limitations to exchanging information and the use of data mining in the early stages of an investigation. The determining factor in deciding whether the application of data mining is legitimate is the possible infringement that its application may have on the privacy of individuals.

The use of data mining is especially relevant in the phase of the exploratory investigation and criminal intelligence investigation. In this phase of an investigation there is still no concrete evidence of a crime or a suspect, so pattern-based inquiries are most likely to be used. However, during an exploratory investigation pattern-based inquiries tend to be far more focussed, and unlike the use of data gathering and data mining for the execution of the normal police task, they are oftentimes aimed at discovering potential suspects. A common approach is to use pattern-matching, a practice commonly referred to as *Rasterfahndung*. The name stems from pattern-based inquiries that were used by the German authorities in the 1970s to track down members of the *Rote Armee Fraktion* (RAF). The German authorities had profiled RAF terrorists and established that certain behavioural patterns indicated a higher likelihood of belonging to an RAF cell (for instance, paying both the rent and electricity bills in cash).

Agent technology does not change the nature of a *Rasterfahndung* exercise itself, rather it alters the scope, effectiveness, and possibly duration of a *Rasterfahndung* exercise. The most important contribution that agent technology can deliver is the easy integration of public-sector and private-sector databases. The fact that software agents enhance the flow of data between public and private databases means that the exploratory investigations in the Netherlands and the criminal intelligence investigations in the United States can be made broader in scope. Moreover, a broader scope means that more criteria can be

incorporated in the data-mining process, possibly making it more accurate, but also more invasive.

In the Netherlands, the ability to use *Rasterfahndung* during an exploratory investigation is restricted by the law of criminal procedure and the Police Files Act. When *Rasterfahndung* includes matching of suspicious behaviour to individuals, the rules associated with informational privacy apply. However, the recently proposed anti-terrorism bill introduces an additional article (126hh CCP) that allows far reaching use of *Rasterfahndung* in the case of an exploratory investigation into terrorism.[4] With a writ from the examining magistrate, the public prosecutor can issue a warrant to any third party demanding data that can be used for *Rasterfahndung*. The article states that any database, both public and private, may be matched. Apart from the procedural demands for a writ from the examining magistrate, procedural safeguards are, in my opinion, minimal. Paragraph 3 of article 126hh only states that "the processing of data is carried out in such a manner that the protection of the personal sphere is safeguarded to the best possible extent", except the demand for a written report of the data mining exercise *ex-post* (paragraph 4, 126hh CCP), concrete procedural safeguards are not given.

In the United States the power of automated information gathering and data mining is also recognised. In essence, the GENESYS project of the Total Information Awareness Office was supposed to be one great *Rasterfahndung* exercise. While privacy safeguards were considered, the law concerning surveillance and privacy itself provides few protection mechanisms that would mitigate any threats to privacy made by GENESYS. While the GENESYS project has been discontinued, the use of advanced data mining is still contemplated in the United States.

In the United States information gathering and the use of data mining is governed by the general rules regarding surveillance and privacy as described in chapter 5. Under the *Attorney General's Guidelines*, the FBI is authorised to use 'information systems' for counterterrorism purposes even in the early stages of an investigation, this could also include *Rasterfahndung* exercises.[5]

In the light of agent technology the current legislation in both the Netherlands and the United States has two important flaws: (1) they do not accurately limit the scope of a data-mining exercise, and (2) they do not pose a limit on the duration of a data-mining exercise. This can be attributed for a large part to the fact that current legislation is adapted to current data-mining technology, where it is still necessary to create a data warehouse from selected datasets. It is my belief that through distributed data mining made possible by agent technology the whole data-mining process will become far more flexible.

4 Parliamentary Series II, 30 164 nr. 2.
5 <http://www.politechbot.com/p-04012.html>

In a distributed data-mining scenario agents could mine any number of public-sector and private-sector databases in real-time.[6] As such, the use has no direct control over the data that is selected for the data-mining exercise. Moreover, software agents can be assigned almost permanently to a particular database and search for relevant information.[7] Thus, in theory, agent technology makes it possible to gather data continuously, much like a wiretap or the FBI's controversial CARNIVORE system for an indefinite period.[8] This would seriously differ from current data-mining exercises.

So, we may conclude that the first legal issue that is raised by the increased effectiveness of data exchange and data mining is as follows: the legal framework is based upon traditional methods of data mining and any safeguards are also based upon these methods. It is my opinion that software agents will influence the way in which data is exchanged and mined to such an extent, that additional safeguards need to be put in place that are more closely related to agent-enabled data mining.

Moreover, we may conclude that a second legal issue is related to the possible panoptic effects associated with data mining. While it might be true that possible panoptic effects of data mining are recognised by the government, there are no safeguards in current surveillance law that limit possible panoptic effects.

8.3.3 System integration

One of the strengths of agent technology is its ability to facilitate the integration of (previously) discrete surveillance systems. From a legal point of view the integration of discrete surveillance systems is problematic since integration can lead to a 'new' surveillance system that is more effective than the sum of its constituent parts.

A first legal issue related to system integration is that while the right to privacy in itself is technology independent, the legal framework that further defines the scope and application of privacy protection is oftentimes technology dependent. Most notably in the area of criminal procedure, the legal framework is usually tailored toward specific surveillance technologies, such as wiretaps, bugs, or cameras. This holds true for both the legal framework of the Netherlands and that of the United States.

---

6 Provided they have the authorisation to access these databases.

7 One could imagine that the mining agent would automatically serve a warrant to a data controller agent situated on the database platform, thus further automating the surveillance process.

8 CARNIVORE, which was later renamed to DCS-1000 is an FBI internet surveillance system that automatically filters data traffic for evidence related to a suspect. The system was named CARNIVORE as it would only target the 'meat' of the communication, i.e., information relevant to a criminal investigation.

A second legal issue related to system integration are the possible panoptic effects of system integration. As of yet it is unclear how people will react to an integrated surveillance system that is active for twenty-four hours a day and extends to much of their daily lives. In both the Netherlands and the United States possible panoptic effects of surveillance resulting from system integration are not explicitly taken into account by the legal framework. Other than by placing limits on the use of surveillance methods, possible panoptic effects are not addressed in both countries.

8.3.4 Empowering surveillance operators

The rules that surveillance operators have to abide by and the investigative powers to conduct electronic surveillance granted to law enforcement officers, are closely related to the state of surveillance technology. The authority vested in a surveillance operator or law enforcement agent is closely linked to the capacity of that operator or agent to conduct surveillance tasks. Furthermore, the authority to use investigative powers is dependent on the effectiveness of the investigative method used and its overall impact on privacy and individual liberty. In general, we may establish the following rule: the more powerful the surveillance tool, the stricter the rules that apply to its use.

The first legal issue we can identify when it comes to empowering surveillance operators is that it is unclear what the authority of surveillance operators and law enforcements officers to use software agents is. When agent technology makes surveillance operators and law enforcement officers more effective, the legal framework should reflect this. As of yet this is not the case, since surveillance operators and law enforcement agencies do not yet use agent technology extensively.

The second legal issue that can be mentioned are the possible panoptic effects of more powerful surveillance operators and law enforcement officers. Once again, we see that the legal framework does not provide any clear answers to this issue, since the panoptic effects of surveillance are currently limited.

8.3.5 Replacing surveillance operators

When agent technology is used by surveillance operators and law enforcement officers they become more effective, and as a result surveillance will be more effective. Moreover, it is possible to replace them by software agents altogether, which makes surveillance more complete, as we have established in sub-section 7.1.4. Therefore, from a legal point of view, this issue bears much resemblance to that discussed in the previous section. Once again, we have a situation where rules and authorities that are based (in part) on the technical limitations

of surveillance (in this case human limitations, such as attention span and limited computational ability) might also apply to surveillance executed by software agents that do not have the aforementioned limitations.

A second legal issue we can mention in this context is, once again, the possible panoptic effects of agent technology. As is the case with all the other quantitative effects of agent technology, possible panoptic effects of replacing surveillance operators are not accounted for in the legal framework.

8.4 Legal issues related to qualitative effects

The legal issues that arise as a result of the qualitative aspects of agent technology pose great challenges to lawmakers and policymakers. Since the private sector is an early adopter when it comes to the application of agent technology, most scholars are examining the legal issues related to software agents in the context of private law.[9] Less attention is devoted to the use of agent technology for surveillance purposes. Therefore, we must examine the legal framework for the protection of privacy and liberty in the light of criminal law more closely. Several important legal issues flow forth from the qualitative effects of agent technology. In this section I shall explore the legal issues that flow forth from the qualitative effects of unclear competency and authority, emergent behaviour, the lack of transparency and insight, adaption, and the strength of the agent metaphor.

8.4.1 Legal status and qualification of investigative powers

In the law of criminal procedure of both the Netherlands and the United States there is no specific mention of agent technology as an investigative method or power. While it is by no means mandatory to codify the use of every investigative method in the law of criminal procedure, it is my opinion that certain applications of agent technology need a statutory basis. In this respect it is particularly relevant to clarify the legal status of software agents in the law of criminal procedure.

As can be judged from section 2.10, the debate on the legal status of software agents is primarily focused on private law. However, with regard to the problem definition of this thesis, questions about the legal status of software agents in the light of law enforcement and national security are more relevant. As mentioned in section 7.2, the autonomy, emergent behaviour, adaptive capabilities, and mobility of software agents raise questions with regard to the legal competence and authority of software agents to undertake surveillance tasks with little or no human supervision. While software agents may have

9 See for instance: <http://www.lea-online.net/>

the technical capacity for autonomous operation, it begs the question whether they also have the legal competence and authority to do so when it comes to surveillance. As long as this question remains unanswered, privacy and liberty might be at risk due to legal uncertainty. In particular in those cases where software agents take over the tasks normally executed by law enforcement officers it is necessary to clarify the role and place of software agents. In order to fulfil their tasks law enforcement officers are endowed with certain powers unavailable to ordinary citizens. The law of criminal procedure limits the use of these powers. A software agent can assist in the tasks of surveillance operators and law enforcement agents, or it can take them over entirely. Currently it is unclear whether the use of agent technology falls within the scope of existing investigative powers, or that new ones need to be created that are specifically tailored towards the use of agent technology as an investigative method. Uncertainty with regard to the legal status of agent technology and the legal qualification of investigative methods in criminal procedure will threaten privacy and liberty. In this context particular issues are raised by emergent behaviour and software agent adaptability.

When we look at the current breed of surveillance technologies we can establish that they do not have the power to adapt. Consequently, the impact of investigative methods can be established rather clearly and rules regarding their use drafted accordingly. However, when an investigative method can change and improve itself thereby becoming a more effective investigative method, the task of defining the investigative power becomes less straightforward. This raises serious questions as to the authority given to an autonomous agent. In turn, this will lead to questions about (1) how may they be used and (2) what limits should apply. In the current legal framework of both the Netherlands and the United States we find no answers to these questions.

The emergent behaviour sometimes found in multi-agent systems could also raise questions about the legal status of software agents and the qualification of their use as an investigative method. Emergent behaviour might lead to unexpected or unintended effects in the application of agent-enabled surveillance. Some of these effects may threaten privacy or individual liberty. Within the current legal framework the possibility of emergent behaviour is not anticipated.

The use of a potent investigative method such as agent technology without a clear basis in the law is unacceptable in my opinion. When there is a clear basis in the law of criminal procedure it will become possible to regulate and, where necessary, limit the use of agent technology. I shall discuss the issue of use limitation in sub-section 8.4.4.

8.4.2 Jurisdiction

Organised crime and terrorism are not limited to national borders. In particular the internet has contributed greatly to the 'globalisation' of crime. In theory, the autonomy and mobility of software agents enables them to query any compatible database or other information source connected to the internet.[10] The fact that software agents can query any number of databases throughout the world could raise questions with regard to jurisdiction. Therefore, the issue of jurisdiction is relevant in the discussion on the use of agent-enabled surveillance.

8.4.3 Transparency

Advanced software agents are highly complex and can act autonomously. This can make their behaviour difficult to predict. Moreover, keeping track of their actions is a daunting task. This potential lack of transparency can cause problems with regard to the foreseeability of software-agent operation. Furthermore, a lack of insight can cause problems when it comes to the accountability of agent-enabled surveillance.

From an information-gathering and data-mining perspective the main issue is that when agent technology is used, it becomes more difficult to establish where data is collected and how it is used. With current information-gathering and data-mining technologies it is relatively clear how data is aggregated and integrated. The current approach to data mining is to take two or more discrete data sets and integrate them in a data-warehouse. Through agent technology this process could become far more flexible. Agents could query any number of databases and establish on the spot whether they contain information worthwhile to law enforcement, and then download the information to a single data repository for mining. Without proper mechanisms for establishing which databases are accessed and which information is being used, the use of agent technology will lead to legal uncertainty due to a lack of transparency. While the current legal framework addresses the issue of transparency and accountability in a number of ways for current surveillance methods and investigative powers, it does not yet do so for agent-enabled data mining.

Issues relating to transparency could also flow forth from the adaptability of software agents and the possible emergent behaviour in multi-agent systems. When it comes to adaptability, a lack of transparency can arise due to the fact that it is unclear what new skills an agent can learn and how these skills will influence its surveillance capabilities. In multi-agent systems emergent behaviour might lead to unexpected behaviour altogether. Within the current legal framework these issues are not yet addressed since adaptability and

10 In practice, access to databases is limited through authorisation procedures.

emergent behaviour are not yet characteristics that any current surveillance method possess. The question then becomes whether the application of advanced agent technology is in accordance with the law. In my opinion their use is not in accordance with current law, since they lack a decent basis in the law, and more importantly, their use does not meet the requisite standards of foreseeability. Therefore, additional safeguards need to be put in place in order to ensure that the use of advanced software agents for surveillance purposes is in accordance with the law.

8.4.4 Use limitation

A fourth legal issue that flows forth from the unclear legal status of agent-enabled surveillance is the problem of use limitation. It is necessary to restrict the use of agent-enabled surveillance to those situations where their use is warranted. As of yet, the law in both the Netherlands and the United States does not describe how rules concerning existing investigative powers apply to agent-enabled surveillance. It is therefore unclear what rules and limitations apply to the use of agent-based surveillance.

As mentioned in sub-section 8.3.3, the more effective the surveillance method is, the stricter the rules that should apply to its use in order to limit any possible negative effects on privacy and individual liberty. Rules governing an investigative method should clearly state how the investigative method should be applied, under what conditions, and in which cases. It is clear that both in the Netherlands and the United States the law of criminal procedure does not meet these criteria when it comes to agent-enabled surveillance.

In subsection 7.1.2 we have discussed more effective data exchange and data mining as a quantitative effect of agent technology. In sub-section 8.3.2 we saw that this quantitative effect (i.e., the increased scope of an agent-enabled data-mining exercise) is not addressed in the legal framework. Apart from a quantitative dimension, the fact that software agents can potentially query any number of public-sector and private-sector databases, also has a qualitative dimension. When it is unclear which data sources an agent addresses for the purpose of a data-gathering or data-mining exercise, its effects on privacy and liberty become difficult to predict and control. This situation becomes even more alarming when an agent has the ability to adapt itself.

In subsection 8.4.1 we already discussed the issue of adaptation in relation to authority. There we saw that any surveillance method that adapts to its environment is more difficult to qualify in the law. This also means that defining the scope of their application is hard, which makes setting borders a difficult task. Classic investigative methods such as wiretaps are currently quite fixed applications, in other words, their scope or impact does not change over the course of their application. With agent technology this could well be different. Software agents that have the ability to adapt to their environment

and learn from their experience become more potent investigative tools over time. Currently, the law of criminal procedure in both the Netherlands and the United States does not accommodate for this possibility and changes are thus necessary.

An analogous problem is posed by multi-agent systems that display emergent behaviour. Since it is hard if not impossible to predict emergent behaviour, it is equally difficult to set boundaries for the use of multi-agent systems in the context of surveillance. Within the current legal framework of the Netherlands and the United States there is no mention of surveillance methods that can display emergent behaviour, as there are no such systems yet in existence. However, when such systems do come into existence it will be necessary to account for the possibility of emergent behaviour within the legal framework.

8.4.5 Strength of the agent metaphor

At this time it is difficult to establish the influence of the agent metaphor on the behaviour of groups and individuals. While it is possible that the agent metaphor contributes to the panoptic effects of agent-enabled surveillance, the idea remains rather speculative. Moreover, if it turns out that the agent metaphor contributes to panoptic feelings experienced by groups or individuals, it is questionable whether a solution to this problem can be found in the law. In my opinion there are no solutions of a legal nature that can address this issue (apart from limiting the use of agent-enabled surveillance). Therefore, I shall not include this qualitative effect of agent technology in the discussion about possible changes to the legal framework.

8.5 The legal framework evaluated

When we look at the legal issues related to the use of agent technology as described above, we may start to draw some general conclusions about the legal issues surrounding quantitative and qualitative effects and their impact on the legal framework. Based on this assessment I shall describe how I feel the right to privacy should be interpreted within the light of these conclusions.

8.5.1 Quantitative effects

The quantitative effects of software agents on surveillance are generic in nature, in other words, the quantitative effects caused by software agents could also be caused by other surveillance technologies. As described earlier, the use of agent technology will mainly constitute a change in the scale of surveillance

rather than in the nature of surveillance. Therefore, I shall not discuss the impact of the individual quantitative effects on the legal framework, but rather make some general remarks about their effects as a whole.

As I have illustrated through a metaphor, a sizeable change in the scale of surveillance can have a profound impact on privacy and liberty. When we accept Bacon's maxim 'knowledge is power' as a valid statement, the use of data is directly linked to the distribution of power within society. By using agent technology data will become more manageable and will be more easily converted to information and knowledge. So, by using agent technology data will become a more valuable source of knowledge for those who control it. It is therefore my opinion that the effectiveness of a surveillance method should be taken into account when judging whether or not the legal framework is still adequate.

However, dealing with the legal issues related to quantitative effects is difficult as they present us with a 'Sorites paradox'. The Sorites paradox (also known as the 'little-by-little argument') is a class of paradoxical arguments that arise due to indeterminacy surrounding the limits of the application of the predicates.[11] The classic example of a Sorites paradox is that of a heap.[12] Because the definition of a heap does not set any clear boundaries as to what must be considered 'a heap', the predicate 'is a heap' is indeterminate. Since the predicate is indeterminate, it is impossible to establish which exact grain makes the difference between 'is not a heap' and 'is a heap'. Given that a single grain is not a heap, it can be argued that by adding a second grain there is still no heap, and by adding a third one there is still no heap, and by adding a fourth there is still no heap, et cetera, et cetera. Ultimately it would seem that since no single grain can make the difference between 'is a heap' and 'is not a heap', we would never get a heap. Conversely, by subtracting one grain from a heap, we still have a heap, by subtracting another grain we still have a heap, *et cetera*. Eventually, by subtracting a grain from the final two grains we arrive at the conclusion that a single grain is also a heap, which is clearly incorrect.

Since there is no clear definition of the predicate 'an acceptable level of privacy and individual liberty' and the effectiveness of surveillance technology (part of which can be contributed to agent technology) rises gradually and not in big steps, we cannot determine what increase in the effectiveness of surveillance technology constitutes a shift from 'is an acceptable level of privacy' to 'is not an acceptable level of privacy'. The problem of the 'surveillance sorites paradox' is therefore closely related to that of the 'slippery slope'. In the debate about (electronic) surveillance, the argument of the slippery slope is often invoked. By a slippery slope we mean that by approving

11 For more information about the Sorites paradox and argumentation see Read (1995) and Verheij (1996).

12 The Greek word for heap is 'soros'.

decision A, which in itself maybe sound, we increase the chance of bringing about decision B, which we oppose. The idea is that gradual increases in surveillance which may in themselves be acceptable will ultimately bring about a total surveillance society which is wholly undesirable. The indeterminacy surrounding concepts such as privacy and liberty makes it easier to slide further down the slippery slope. The issue of the surveillance sorites paradox in conjunction with the problem of the slippery slope, makes regulating the use of surveillance technology difficult. While this paradox makes it difficult to determine accurately the exact time at which the legal framework becomes inadequate, I believe that we can determine already that due to the arrival of agent-enabled surveillance the current legal framework *will* become outdated at some point in time.

In my opinion there are three separate but interrelated causes to the fact that the current legal framework for the protection of privacy and individual liberty will no longer be adequate in the near future, namely, (1) there is too much focus on secrecy and concealment in the phase of data gathering, (2) there is too much focus on *personal* data in data protection law, (3) and there will be an even stronger move from reactive to pro-active investigation as a result of new surveillance technologies such as software agents.

Focus on secrecy and concealment in the phase of data gathering

As I have explained in chapter 5 many of the social and psychological functions of privacy hinge on the idea of concealment. For instance, through secrecy and anonymity we can create a space for emotional release and self-evaluation. Furthermore, concealment of sensitive information about our person protects us against involuntary disclosure of this information. While shielding the individual from outside influences is one of the fundamental functions of the right to privacy, it is interpreted somewhat different in the context of surveillance. Here, the primary goal of the right to privacy is predominantly that of safeguarding an individual's autonomy, and not their right to 'seclusion'. The goal of the legal framework in the context of surveillance is for the most part creating a sphere of autonomy for the individual by means of concealment. When we take a look at the current laws on surveillance in both the Netherlands and the United States we can establish that there is a strong focus on hiding or concealing data from the government for this purpose.

A first problem with the idea of concealment is that while most people agree that it is legitimate to hide information from others in certain contexts, secrecy and concealment do carry a certain negative connotation with them. Oftentimes information uncovered over the course of a criminal investigation is burdening for the suspect. In some cases however, the right to privacy prohibits the use of such information. In particular in high-profile cases such as murder or terrorism cases, the right to privacy is then seen as an obstacle instead of a basic human right and a necessity for the functioning of the individual and society as a whole. This, of course, gives privacy the 'bad

publicity' mentioned earlier, and compels law enforcement officials into making statements such as *'privacy is the hiding place of evil'*. Moreover, when we view the interest of the individual and balance it with the interests of society as whole, it is not difficult to predict that the legitimate privacy interests of individuals are most often subordinate to the interests of society as a whole. The metaphor of balance has led to the ideological choice being presented as privacy *or* security (see, for instance, Etzioni 1999). However, security and privacy are not dichotomous rivals to be traded one for another, rather they are dual objectives, each to be maximised within certain constraints (Taipale 2003, p. 25).

A second problem with the idea of concealment is that hiding information is becoming evermore difficult in the information society. When we study the legal framework for surveillance and privacy and the accompanying case law, we can determine that a reasonable expectation of privacy criterion (which flows forth from the secrecy paradigm) is still the primary test to determine whether violations of privacy have occurred over the course of a criminal investigation in both the Netherlands and the United States. As I described previously, the reasonable expectation of privacy criterion is put under pressure by technological developments and the move towards ambient intelligence. The quantitative effects of agent technology will only add to this ongoing development. For instance, can it be said you have a reasonable expectation of privacy while chatting if you have the knowledge a software agent could be monitoring your chat session? Or, do you have a reasonable expectation of privacy knowing that software agents could be monitoring the dataflow going into and out of your networked home? These examples illustrate that software agents will undermine the reasonable expectation of privacy even further. Rapid advances in surveillance technologies make it so that people can no longer maintain any reasonable expectations of privacy. In that sense Nealy was not entirely wrong when in 1999 he made the statement: "You have zero privacy anyway, get over it". However, in my view the question is not whether an individual should be entitled to privacy solely on the basis of his (reasonable) expectations thereof, but rather on a decision on how invasions of privacy influence the balance of power between the watchers and the observed. Such a decision goes beyond the individual but must be viewed in a broader context. In a sense, the reasonable expectation of privacy is only the means to a greater goal, *viz.* liberty. However, it is based on an old-fashioned conception of privacy that can no longer be maintained in the information society. So, while the ideas behind the reasonable expectation of privacy are sound (i.e., creating a sphere of autonomy) the practical application is flawed. Thus, in the future the legislator, but more importantly the judge, should move away from the reasonable expectation of privacy criterion as the primary means of considering whether an invasion of privacy is legitimate.

It begs the questions whether the right to privacy in its current conceptualisations (*viz.* the secrecy paradigm and informational privacy) is actually the most effective approach to safeguarding individual liberty. As described in chapter 6, there are a number of issues with the current conceptualisations of the right to privacy in the information society, which render it less than optimal for the (complete) protection of privacy and liberty in my opinion. The shortcomings of the right to privacy are reflected in the structure of the legal framework with its focus on secrecy, concealment, individuality, the distinction between the public and the private, and the preoccupation with personal data. Due to the predominance of the secrecy paradigm and the idea of informational privacy in contemporary privacy discourse, both the legal systems of the Netherlands and the United States have difficulty in keeping up with the rapid changes in technology. I believe that the use of agent technology will place additional strain on this ageing model for privacy protection.

Focus on personal data in data protection law

Since privacy is by definition an individual right, it seems logical to focus its application on the processing of *personal* data. Both in the Netherlands and the United States the protection of informational privacy is therefore based on the notion of an identifiable person. However, I believe that this approach is less than satisfactory when it comes to defending liberty. The reason for this is that encroachments upon liberty resulting from extensive data processing can also occur when there is no identifiable person. This is the first problem with a focus on personal data in data protection law.

A prime example of this problem is the exercise of *Rasterfahndung*. In my opinion *Rasterfahndung* carries with it certain risks to constitutional rights that cannot be easily mitigated by the right to informational privacy. The greatest risk *Rasterfahndung* poses to constitutional rights is the chance of 'racial profiling'. It is not uncommon in surveillance practice that surveillance is aimed at certain groups disproportionately, based on, for instance, their ethnicity, religion, or political preference. Due to the fact that *Rasterfahndung* is based on predefined risk criteria it is likely that certain groups will be subjected to this particular data-mining exercise more often than other groups. A simple example to illustrate this is a pattern-based inquiry into international terrorism. It is likely that such an inquiry will include information regarding religious preferences (i.e., being a muslim), which could encroach upon the freedom of religion. Furthermore, *Rasterfahndung* can also bring with it panoptic effects associated with extensive data integration. In order to avoid that profiled people could refrain from engaging in activities associated with risk, this chilling effect on individual liberty will be enhanced through agent-enabled data mining.

A second problem with a strong focus on personal data is that it is becoming increasingly hard to determine what personal data is in the ambient

intelligence paradigm. Personal data is described in article 2, paragraph A of the European Data Protection Directive (95/46/EC) as: "any information relating to an identified or identifiable natural person". So, in order for data protection law to apply the processed data must be able to identify a natural person either directly or indirectly. With a lot of the data processed in the ambient-intelligence paradigm it is not clear whether they must be considered personal data.[13] In the ambient-intelligence paradigm we will leave 'electronic footprints' to an increasing extent, but it is unclear whether all of these footprints may be considered personal data (Terstegge 2006, p. 39). However, much like personal data, these electronic footprints can be used to influence groups or individuals. A good example is traffic data and the issue of data retention. While traffic data in itself is not personal data (only once it has been linked to user data) it can still be used for investigative purposes. This might lead to panoptic effects that have a negative influence on liberty from which data protection law will not shield us.

While it is important to regulate the use of personal data through the existing data protection law, it is my that opinion we have to shift our attention towards the way in which constellations of data (whether personal data or not) are being used and how this use affects (individual) liberty within our society. We must acknowledge the fact that the uses of (agent-enabled) data mining do not only threaten privacy, but also other human rights, such as the freedom of speech and the freedom of association. Moreover, the extensive use of data mining focused at particular groups within society could be detrimental to social cohesion and constitute a violation of the right to equal treatment under the law.

Towards pro-active investigation, monitoring, and control

Technology promises to enable law enforcement agencies to spot a potential crime in an earlier stage, possibly avoiding it altogether. In the legislation of both the Netherlands and the United States we can therefore clearly discern a move from reactive investigation towards pro-active investigation, monitoring, and control.[14] This is particularly true for anti-terrorism purposes. Due to the pro-active approach towards investigation, surveillance is applied in an earlier stage. Because there is no individualised suspicion much of the pro-active investigation takes place in the public space.

Monitoring of the public space (both physical and virtual) is becoming increasingly prevalent each day. In the physical world CCTV cameras are only the first step towards pervasive and ubiquitous sensor networking in the public space. The COMBAT ZONES THAT SEE program offers us a first glimpse into the future of surveillance in the public space. The XENON application offers a

13 A good example of this problem is RFID: should we consider the data stored in an RFID-tag as personal data?

14 See for a discussion of this phenomenon: Moerings 2006 and Cleiren 2006.

similar glimpse into the future of online surveillance. Part of this development is driven by agent technology.

When we examine the current legal framework for the Netherlands and the United States we can establish that monitoring of the public space is hardly limited in the legal framework by the right to privacy. This is not surprising since the public sphere is the opposite of the private sphere. So, while investigative methods, such as wiretapping, the use of undercover agents, and the use of pen registers and trap and trace devices, are strictly regulated, monitoring of the public space is not. The reason for this is that monitoring of the public space is seen as unobtrusive. As we have seen, software agents are particularly adept at unobtrusive monitoring. It might then seem that agent-enabled surveillance does not pose a great threat to privacy and individual liberty. However, we can judge from the legal issues surrounding the quantitative effects of agent technology that monitoring of the public space through agent technology could trigger panoptic effects that are normally associated with invasions of privacy.

8.5.2 Qualitative effects

Unlike the legal issues associated with the quantitative effects of agent technology, the legal issues related to qualitative effects can be clearly linked to the specific characteristics of agent technology. The qualitative effects of agent technology thus trigger legal issues that are unique to agent-enabled surveillance, which makes identifying potential shortcomings in the current legal framework easier. I have enumerated the most important of the legal issues and the accompanying shortcomings in the legal framework in section 8.4.

When we evaluate the legal issues related to qualitative effects in the light of the current legal framework we can establish that in order for the legal framework to remain effective, changes must be made. The legal issues that arise out of the qualitative effects can be contributed to the specific characteristics of agent technology, most notably autonomy, adaptability, and emergent behaviour. The uniqueness of these characteristics will force us to amend the current legal framework. The legal issues identified in section 8.4, *viz.*, (1) the legal status and qualification of investigative powers, (2) jurisdiction, (3) transparency, and (4) use limitation will prompt changes to the legal framework.

Agent characteristics such as autonomy, emergent behaviour, and adaptability deserve some specific mention in this section. We find these characteristics pre-dominantly in advanced agent applications, of which the development is still in the very early stages. As we have seen in chapter 2, advanced software agent applications will most likely not see broad deployment before 2010. While changing the legal framework in this stage of the development is unnecessary and possibly counterproductive, we should start a *discussion* on the

ways in which the legal framework should be changed already given the slow responsiveness of the law to technological changes. Particularly important shortcomings in the legal framework that need to be addressed are the legal status of software agent-enabled surveillance applications and the limits of their use.

Apart from the legal issues related to the legal status of agents and the limits of their use, issues related to transparency and jurisdiction must also be resolved. These issues will most likely only arise in open systems. I shall discuss possible solutions to this issue in the next chapter. With regard to the issue of transparency, systems that are totally open pose serious difficulties. Oversight and accountability, for instance, are not easily realised within these systems. I shall discuss some possible solutions in the next chapter.

Taking the various legal issues related to qualitative effects into account, we arrive at the conclusion that without amendments to the current legal framework the use of agent-enabled surveillance will in large parts exist within a legal vacuum. In other words, without changes to the legal framework, legal certainty is at risk. Moreover, the use of agent-enabled surveillance methods will not be in accordance with the law since they lack the requisite foreseeability, a requirement that is particularly important in Dutch law.

8.6 Provisional conclusions

While the effects of agent technology on surveillance may not be readily apparent at this stage, it is my belief that advances in the development of agent technology will have profound effects on surveillance in the near future. It is likely that agent technology will seriously enhance the capabilities of surveillance operators, something that will impact the legal framework. It is my conclusion that these effects will influence the legal framework in two distinct ways: (1) they will put additional pressure on the sustainability of the current conceptualisations of privacy (the secrecy paradigm and personal data protection), and (2) they will generate a need for new legislation governing the use of advanced software-agent applications.

1 The quantitative effects of agent technology in conjunction with other developments in information and communication technology (culminating in the idea of ambient intelligence) will eventually change the nature of surveillance as a whole. Such a change needs to be reflected in the legal framework for the protection of privacy and (individual) liberty.

2 The unique characteristics of agent technology could have a profound impact on surveillance, privacy, and liberty. If this is the case, I feel that it is necessary to regulate the use of at least the particularly potent agent-enabled surveillance applications. While a software agent might be con-

> sidered an investigative tool that simply aids law enforcement in the exercise of their official tasks, I feel that in many cases such an approach is not realistic. Potent software agent applications (for instance, adaptable software agents that have high levels of autonomy) might influence privacy and liberty to such a degree, that a specialised regime should apply that provide appropriate safeguards. Such a regime should find a place in the law, preferably in the law of criminal procedure.

When we examine the likely effects of software agent-enabled surveillance on the legal framework we can determine that without changes it will be unable to fulfil the functions of the law as enumerated by Van Hoecke (2002).

One of the primary goals of the law is to structure society. We have seen that software agents used for surveillance purposes can upset the balance of power between the watchers and the observed when the law does not limit their application. Without proper safeguards, most of which are not available in the current legal framework, agent-enabled surveillance will threaten both negative and positive liberty. Thus, without changes to the legal framework, agent-enabled surveillance will undermine the law's ability to structure political power. Moreover, agent-enabled surveillance may threaten social cohesion when their use is aimed at certain groups disproportionately.

While agent-enabled surveillance may bring about desirable behaviour, it can also have serious panoptic effects. We have seen that the current legal framework is equipped less than optimal for the creation of spheres of autonomy in the context of agent-enabled surveillance, which is primarily due to a pre-occupation with the right to privacy. So, in order to minimise any excesses in the bringing about of desirable behaviour, we must find new ways of guaranteeing spheres of autonomy.

In the next chapter I shall discuss some possible changes to the legal framework that should aid in keeping the legal framework up to date.

9 An enhanced legal framework

The price of freedom is eternal vigilance
Thomas Jefferson

In chapter 7 we examined the ways in which agent technology might influence surveillance, privacy, and liberty. In chapter 8 we established how these changes could impact the legal framework for the protection of privacy and (individual) liberty in the area of electronic surveillance. In this chapter I shall give my view on what changes should be made to the legal framework in order for it to provide more protection against possible negative effects of agent-enabled surveillance. However, merely changing the legal framework is insufficient: the rules set forth by the legal framework must be implemented in technology and in procedures to make them effective. Therefore, in this chapter I shall discuss how possible changes to the legal framework in combination with technology and procedures can contribute to maintaining privacy and liberty.

Before we turn our attention to the task of dealing with the individual quantitative and qualitative effects of agent-enabled surveillance, I shall discuss some general considerations concerning agent-enabled surveillance and the law in section 9.1. Next, I shall discuss possible solutions to the individual quantitative and qualitative effects (both changes to the legal framework and their implementation in technology and procedures) in sections 9.2 and 9.3, respectively. Since the actual use of (advanced) agent applications for surveillance purposes is still in its infancy and details about the actual implementation are thus lacking, I shall not formulate the legal provisions precisely. Rather, I shall provide starting points for a future discussion about agent-enabled surveillance and the legal framework. I shall give my opinions on the future for agent-enabled surveillance in section 9.4. A summary of findings and opinions shall be given in section 9.5.

9.1 General considerations

Before we start discussing possible legislative reactions to the quantitative and qualitative effects of agent-enabled surveillance, some general considerations must be taken into account. These considerations deal with the requirements

for the legal framework, the role of technology, and the scale and effectiveness of electronic surveillance in the (near) future.

9.1.1 Requirements for the legal framework

The development of agent technology for surveillance purposes is not an isolated event. In general, there is a strong trend towards the development of electronic surveillance tools, in particular for anti-terrorism purposes. Moreover, there is a trend visible in both the Dutch and the United States criminal justice system towards pro-active investigation of organised crime and terrorist activities. Terrorism in particular is seen as such a great threat to (national) security that new provisions in both substantive criminal law and the law of criminal procedure have been introduced in both the Netherlands and the United States. These new provisions have broadened the range of persons that can be subjected to surveillance while at the same time the conditions under which electronic surveillance may be used have been relaxed. While this is not the direct result of international terrorism, since the trend was recognisable before the September 11 attacks, the fear of international terrorism has definitely contributed to the process.

Taking this into consideration, there are some important general requirements that the legal framework must meet when it comes to agent-enabled surveillance. If these requirements are not met privacy and liberty are at risk, and the legal framework is unable to fulfil adequately the functions set forth by Van Hoecke (2002) (see chapter 8). The requirements are not unique to agent technology; rather they apply to all forms of electronic surveillance and their effects, whether they are of a quantitative nature or a qualitative nature. Furthermore, it must be noted that this list is not an exhaustive list of requirements. However, I do feel that the requirements given below are of particular importance when it comes to agent-enabled surveillance. In my opinion they are: (1) the principle of legality, (2) a clear substantive criminal law, (3) proportionality and subsidiarity, (4) equal treatment under the law, (5) statutory limitations, (6) transparency and accountability, and (7) the right to participation. Most, if not all, of these seven requirements are either explicitly codified in the existing legal frameworks of the Netherlands and the United States, and have been developed in the jurisprudence of the Courts, or they are part of the more general thinking about privacy, liberty, surveillance, and the law. Still, I feel it is necessary to elaborate below on these requirements in the context of agent-enabled surveillance.

The principle of legality

The first requirement is that agent-enabled surveillance must adhere to the principle of legality. This means that the authority to use agent-enabled surveillance must have a statutory basis in the law of criminal procedure. While

many investigative methods are not explicitly codified, it is my opinion that some agent-enabled surveillance applications can be so powerful that they require a statutory basis in the law. I shall elaborate on this requirement in subsection 9.3.1.

A clear substantive criminal law

The second requirement for the legal framework is not aimed at the law of criminal procedure but rather at substantive criminal law. We have seen that through changes in substantive criminal law, the scope of criminal liability has been greatly expanded over the past few years. As a result of this development, investigative powers may oftentimes be used in an earlier phase of an investigation. Moreover, they can be aimed at a larger group of individuals. Thus, the room for discretionary authority and errors increases. Moreover, when powerful surveillance technologies are applied for pro-active investigation, panoptic effects can become stronger since 'everybody is a potential suspect'.

Agent-enabled surveillance will make use of the increased room for surveillance thereby further intensifying surveillance and its possible negative effects. For that reason, it is my opinion that substantive criminal law should be sufficiently clear and should leave as little room for discretionary authority as possible. In particular, this should be so when it happens that potent surveillance technologies such as software agents may be employed.

Proportionality and subsidiarity

The application of a particular investigative power must always be judged according to the requirements of proportionality and subsidiarity. These requirements are based on the condition set forth in article 8 ECHR that any interference into a person's private life must be necessary in a democratic society. The principle of proportionality entails that the nature and the extent of the interference must be weighed against the goal it is meant to attain. When the goal justifies the means used (i.e., the interference), the requirement of proportionality is met. The principle of subsidiarity entails that when a less infringing investigative method or power is available this method or power should be used instead of the more infringing one.

Equal treatment under the law

The principle of equality and the prohibition of discrimination is a key element of any civilised nation. The first article of the Dutch Constitution sets forth the principle of equality and prohibits discrimination, while article 14 ECHR does the same at the European level. In the United States the Fourteenth Amendment to the United States Constitution guarantees equal protection under the law and thereby restricts activities such as (racial) profiling.

While the principle of equality and the prohibition of discrimination are fundamental rights, it is my opinion that their relevance in the area of

(electronic) surveillance is underestimated. The process of identification, categorisation, and assessment that is associated with surveillance is essentially a discriminatory process. Therefore, extensive use of surveillance brings with it the risk of discrimination. We have seen that electronic surveillance, most notably data mining, is particularly susceptible to discrimination. Therefore, it is my opinion that surveillance systems and procedures must be regularly screened for signs of discrimination.

Statutory limitations

One can make a compelling case for the extensive use of electronic surveillance. However, as I have described throughout this thesis we should be careful when it comes to extensive application of electronic surveillance. In my opinion restricting the use of agent-enabled surveillance is crucial when it comes to safeguarding privacy and liberty. We can curb the possible negative effects of agent-enabled surveillance by restricting its use in several ways, *viz.* (1) purpose specification, (2) limitation on application areas, (3) limited use as evidence, (4) a limit on the duration of surveillance, and (5) a limitation of the scope.

A first way of restricting the use of agent-enabled surveillance is through a clear specification of its purpose. One of the starting points of the *Special Powers of Investigation Act* in the Netherlands, for instance, is that the use of special investigative powers should be limited to the goal of settling criminal offences in a court. This means that investigative powers may not be used for other purposes, such as improving the intelligence position of the police or dismantling a criminal organisation if this does not lead to settlement by a criminal court. Since agent-enabled surveillance can be easily used for prolonged monitoring activities, I feel this requirement should also apply to agent-enabled surveillance.

A second way in which agent-enabled surveillance could be limited is to exclude certain areas from agent-enabled surveillance. This limitation is especially important in areas where panoptic effects of surveillance could chill activities that are crucial to our democratic society, such as the freedom of speech, political activity, and democratic participation. Therefore, it is my opinion that we should limit the use of agent-enabled surveillance in areas that are primarily concerned with these activities. This is especially important when it comes to pro-active investigation. That is why in the United States the *Attorney General's Guidelines* stipulate that when it comes to investigative efforts in advance of actual criminal conduct:

> "it is important that such investigations not be based solely on activities protected by the First Amendment or on the lawful exercise of any other rights secured by the Constitution or laws of the United States."

A third way in which agent-enabled surveillance could be limited is by excluding certain pieces of surveillance information as evidence in a criminal court. This is especially relevant when it comes to agent-enabled data mining. In pro-active investigative efforts pattern-matching database techniques (such as *Rasterfahndung*) can be used. When through the use of these techniques a suspect is identified we must take care not to view this information as evidence. It is at best an indication on which to base further investigative activities.

A fourth way to avoid possible negative effects of agent-enabled surveillance is to limit the duration of any surveillance task undertaken by software agents. Software agents have the benefit that they can operate for an indefinite period without human supervision. As I have described in chapter 7, this makes surveillance far more powerful than previously possible. In order to limit the power of agent-enabled surveillance time limits should be imposed where possible.

A fifth way in which agent-enabled surveillance could be restricted is by setting boundaries on its scope. By limiting the amount of data sources an agent may access, by excluding certain data sources, and by excluding certain types of data, we can limit the effects of agent-enabled surveillance on privacy and liberty.

Transparency and accountability

Independent scrutiny of government surveillance efforts is essential in a democratic society. Through transparency and accountability we ensure that the protection against surveillance provided by the law is actually effectuated. Accountability is first and foremost realised through judicial oversight of electronic surveillance. Judicial oversight ensures that the proper procedures have been followed when applying investigative powers. In the Netherlands and the United States the law prescribes that in those cases where potentially intrusive investigative powers are used, a surveillance warrant requires both executive and judicial examination. However, the current trend is to reduce the amount of judicial oversight in order to make the use of covert surveillance more efficient and effective. If we are to ensure privacy and liberty in the light of agent-enabled surveillance we must ensure that judicial oversight is maintained.

Also of importance is the accountability of the actual application of agent-enabled surveillance, in other words, what are the actions that an agent has undertaken in the pursuance of its goals. This is more a technological issue, something I shall explore further in subsection 9.3.3.

The right to participation

We have seen that synoptic surveillance can help restore the balance between the observers and the observed persons. Thus, where possible, individuals should be granted insight into what information is being gathered and processed about them and for what purposes.

Such a right to participation already exists in private law. In the Netherlands, the Data Protection Act provides data subjects with a right to participation. However, a right to participation does not exist when it comes to disciplinary surveillance. Since the right to privacy by itself cannot provide the necessary protection against extensive surveillance, I feel it is important that we look beyond the right to privacy and search for new protection mechanisms. In my opinion awareness about surveillance is one of the primary protection mechanisms. As such a right to participation should also be introduced in the area of disciplinary surveillance. Access to information about surveillance should only be blocked in those cases where covert surveillance is deemed necessary for the success of an investigation.

9.1.2 The role of technology

Now that we have discussed some general requirements for the legal framework it is time to examine how these requirements could be implemented in practice. For this purpose, we have to turn our attention to the technology itself. Technology plays an essential role in the discussion about the possible solutions to the negative effects of agent-enabled surveillance. First of all, any changes to the legal framework for agent-enabled surveillance must be effectuated in the technologies and procedures associated with agent-enabled surveillance. In particular, when it comes to the quantitative effects of agent technology, it is not just changes to the legal framework that determine the protection of privacy and (individual) liberty, it is rather how these rules are implemented within the technology and the accompanying procedures. Second, awareness about agent technology and its effects play a key role. As we have discussed in chapter 1, technological turbulence is a characteristic of the information society. When a society is in a continuous state of technological flux, it is difficult for people to keep up with the rapid pace at which technology is developing. Consequently, it is difficult for people to form an informed opinion on the use of agent-enabled surveillance.

Code as Code

Human life is governed by rules: when it comes to our physical environment the laws of nature bind us, and when it comes to human interaction we follow legal rules and obey social norms. Apart from these physical and societal rules, we may distinguish a third category of rules, namely, those laid down implicitly or explicitly in software architecture. Much like the laws of nature, software code determines what is possible and what is impossible within an information system. In this way software code can regulate human behaviour, help enforce the rules of the legal framework, and can regulate the behaviour of the information system itself.

In his book *Code and Other Laws of Cyberspace*, Lessig (1999) argues that software code can regulate human behaviour as effective as any legal rule. Because the architecture of an information system determines the options a user has, it is the architecture that actually sets the rules. These rules can reflect the rules set forth by the legal framework, or they can differ from those set forth by the legal framework. So, when we look at agent technology, the design of software agents and the platforms they operate on should be designed in such a way as to be in line with the rules set forth in the legal framework.

A second way in which software code can help enforce the legal framework is by providing tools that aid in securing the rights granted by the legal framework. In the context of this thesis the so-called privacy-enhancing technologies (PET's) are relevant as well as technologies that enable synoptic surveillance.

Software code can also regulate the behaviour of the information systems themselves. By setting 'behavioural rules' for an information system in the software code, system designers determine how their systems interact with their environment and how they respond to different situations. In the context of software agents these rules are particularly relevant since software agents have the ability for autonomous action. The behavioural rules given to an agent should be coded in such a way that software agents comply with the rules of the legal framework.

Awareness

Throughout this thesis I have described how surveillance technologies influence the balance of power within society. If we examine the role technology plays in regulating human behaviour, it follows that the application of (surveillance) technology can be viewed as a principal factor in the distribution of power within society. Awareness about the role of surveillance technology in society is vital in the discussion about surveillance, privacy, and liberty. It is my belief that a lack of understanding about the application of surveillance technologies will lead to misconceptions about the implications they may have for the distribution of power within society.

Both policymakers and lawmakers should be aware of the effects agent technology has on surveillance and thus on privacy and liberty. When it comes to disciplinary surveillance the issue that must be examined thoroughly is how the use of agent-enabled surveillance influences the balance of power within society. Since knowledge is power, the use of agent-enabled surveillance can shift the balance of power considerably. To counter this threat additional safeguards of both a legal and a technical nature must accompany any new investigative methods and powers. But when lawmakers and policymakers lack knowledge about the (long-term) effects of agent-enabled surveillance they could fail to make the necessary precautions and implement appropriate safeguards.

However, awareness about the role of technology should not be limited to policymakers and lawmakers, but should also extend to the subjects of surveillance. Individuals should become more aware about what agent-enabled surveillance is, how it is used, and how it may impact their privacy and individual liberty. In this way we can prevent many of the negative effects of surveillance, most notably those caused by the unseen panopticon. Moreover, the foreseeability of an investigative measure is a requirement that is a direct consequence of article 8 ECHR and the accompanying jurisprudence.

9.1.3 Scale, effectiveness, and the legal framework

It is crucial for lawmakers and policymakers to be aware of the fact that there is a move towards an increasing effectiveness of surveillance as a result of agent-enabled surveillance. Currently, surveillance is still in large parts dependent on human efforts. As we have seen in chapter 7, human imperfections lead to a *de facto* protection of privacy and liberty. Software agents can take away many of these imperfections, thereby greatly enhancing the overall effectiveness of surveillance.

Lawmakers and policymakers should recognise this development, and judge the use of agent-enabled surveillance in the light of this broader picture. In my opinion the effectiveness of an investigative method should be taken into account when judging whether it may be applied. This is in line with the opinion of the United States Congress Office of Technology Assessment (1988, p. 51), which stated that: "What is judicially permissible and socially acceptable at one time has often been challenged when technology changes." Thus it will not suffice to state that the use of agent-enabled surveillance is merely a more effective way of using an existing investigative power.

As mentioned in subsection 8.3.4, the authority vested in a surveillance operator or law enforcement officer is closely linked to the capacity of that operator or officer to conduct surveillance tasks. Furthermore, the authority to use investigative powers is dependent on the effectiveness of the investigative method used and its overall impact on privacy and liberty. Thus, the more effective the surveillance method is, the stricter the rules that should apply to its use in order to limit any possible negative effects on privacy and (individual) liberty. These rules should clearly state how the investigative should be applied, under what conditions, and in which cases. It is clear that both in the Netherlands and the United States the law of criminal procedure does not meet these criteria when it comes to agent-enabled surveillance.

The above reasoning is supported by a United States Supreme Court case, that of *United States Department of Justice v. Reporters Committee*. In this case the Court held that the effectiveness of technology to disclose information can

influence the privacy interests in the information at stake.[1] The case dealt with the question whether information organised and stored in FBI 'rap sheets' was considered public information given the fact that the individual pieces of information that made up the rap sheet were previously disclosed to the public.[2] The case centred on a Freedom of Information Act (FOIA) request filed by the Reporters Committee for Freedom of the Press for the disclosure of certain FBI rap sheets. The FBI rejected the request on the grounds that it violated the privacy rights of the person (Charles Medico) mentioned in the rap sheets. The Freedom of Information Act, which is aimed at disclosing government information to the public, contains an exemption (7c) that allows FOIA requests to be denied if the disclosure of information violates the privacy of an individual. The Reporters Committee for Freedom of the Press subsequently filed suit arguing that because the events summarised in the rap sheet had been previously disclosed to the public, Charles Medico's privacy interest in avoiding disclosure of the rap sheet approached zero. The Court however held a different view towards informational privacy and stated as follows.

> "...The issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."

The Court thus acknowledges that the *accessibility* of information is of importance in judging whether information must be considered public or private. We can extend this line of thinking to the use of agent technology by law enforcement. When technology enables an existing process in law enforcement to become far more effective than previously possible, the legal framework that governs that process should be re-evaluated in the light of the new possibilities.

9.2 Dealing with the quantitative effects of agent-enabled surveillance

Now that we have discussed some general considerations regarding agent-enabled surveillance and the legal framework it is time to turn our attention

1 *United States Department of Justice v. Reporters Committee,* 489 US 749 (1989).

2 Rapsheets are criminal identification records maintained by the FBI that contain descriptive information as well as a history of arrests, charges, convictions, and incarcerations.

to the discussion about dealing with the individual quantitative effects of agent-enabled surveillance.

9.2.1 Efficient monitoring and data gathering

In both the Netherlands and the United States the legal framework for electronic surveillance and privacy determines under what circumstances (personal) data may be monitored and gathered by law enforcement agencies. Technological developments that enable law enforcement agencies to gather data more efficiently put pressure on the existing legal framework. We have determined in chapters 7 and 8 that automated surveillance and data gathering, made possible by agent technology, will most likely change the scale and effectiveness of surveillance. As mentioned in subsection 9.1.3 this development may force us to rethink the legal framework as a whole. It is therefore best to recognise the effectiveness of agent-enabled surveillance and data gathering as a quantitative effect of agent-enabled surveillance and address this issue in the broader context of electronic surveillance, privacy, and liberty.

In my opinion agent-enabled surveillance changes the severity of monitoring and data gathering as an investigative method. I feel that this new that reality must be reflected in the legal framework. With regard to the legal framework of the Netherlands this could mean that the use of software agents for online surveillance purposes would fall outside the scope of article 2 Police Act 1993. With regard to the legal framework of the United States it would mean applying stricter rules in the *Attorney General's Guidelines* for automated surveillance.

Furthermore, the fact that software agents can greatly expand the scale on which data can be monitored and gathered, may also force us to limit the scope of their application. We can do so, for instance, by stipulating in the legal framework that it must be sufficiently clear which data sources may be monitored or accessed by software agents. A second way to limit the power of agent-enabled data monitoring and gathering is by explicitly excluding certain sources or types of data. Furthermore, a limit should be placed on the duration of agent-enabled monitoring and data gathering. The best way to effectuate these rules is by programming them directly into the reasoning model of the agent.

When it comes to setting the rules for agent-enabled monitoring and data gathering we must take two different situations into account. The first situation deals with monitoring and gathering data from the internet. Software agents can gather data by accessing data sources on those parts of the internet that are accessible to the public (e.g., webpages, public chatrooms, and newsgroups). Since these data are readily accessible there are currently few procedural requirements that law enforcement must meet before data can be

gathered.[3] Once data has been lawfully gathered the normal rules for using police data apply. The second situation deals with gathering information from sources that are private.[4] If software agents are to collect data from these private sources they must base their actions on specific authorities found in the law of criminal procedure. In the legal framework of the Netherlands and the United States these provisions contain specific procedural requirements. In my opinion software agents must also meet these procedural requirements. For instance, when in the physical world a law enforcement officer makes a demand for private sector data, he must present the data controller with a warrant. The same rules should apply to software agents. To ensure the agents rightfully obtain private sector data they must identify themselves and provide proof of their authority (for instance, by presenting a digital warrant).

9.2.2 Effective data exchange and data mining

Since the power of agent-enabled data mining is evident, we must ensure that the law restricts excessive use of this technology. Currently, the legal framework in both the Netherlands and the United States set forth the rules for data-mining exercises by law enforcement agencies. When it comes to regulation in the area of data exchange and data mining we arrive at roughly the same conclusion as we have seen in the previous section on agent-enabled data monitoring and data gathering. When the effectiveness of agent-enabled data mining surpasses that of traditional data mining it may be necessary to rethink the legal framework as a whole.

One quantitative effect of agent-enabled data exchange and data mining that should definitely be taken into consideration is the ease with which information sources can be linked and integrated. Oftentimes there is no need for extensive data-mining exercises but rather targeted searches in different distributed databases. The easy accessibility of information made possible by agent-enabled data-exchange will have a significant impact on the effectiveness of surveillance, and will facilitate the use of subject-based inquiries. In particular in the United States where private-sector databases are readily accessible by law enforcement agencies, this development is significant. In addition, the fact that the Patriot Act, for instance, sanctions the free exchange of data between law enforcement officers may lead to a situation where the increased accessibility of information could have considerable consequences for privacy and liberty. Recent legislative changes in the Netherlands have also increased the accessibility of private-sector databases. Therefore, lawmakers and policy-makers should reconsider whether the current legislative framework provides adequate protection in the light of this development. If not, legal barriers need

3 Also see subsection 9.3.3.

4 In this situation the automated monitoring of data is less relevant.

to be erected to prevent the further integration of databases and curtail an agents 'freedom of movement'. By placing limits in the legal framework on which databases may be accessed and integrated by agents, we create artificial barriers that reduce the accessibility of information.

Apart from setting artificial barriers in the legal framework to reduce the accessibility of information, there are several techniques that can mitigate possible negative effects of agent-enabled data mining. Taipale (2003) gives a good overview of the three most relevant techniques, *viz*. rule-based processing, selective revelation, and strong credential and audit mechanisms. I explicitly note that these solutions are of a technical nature, not a legal nature.

Rule-based processing

Rule-based processing technologies allow the incorporation into the technology itself of policy judgements as to how, when, where, and for what purpose particular information can be accessed (Taipale 2003, p. 60). An added benefit is that rule-based processing is particularly well suited for implementation in software agents. By using rule-based processing software agents can query distributed databases according to pre-determined rules, and make use of labeled data to ensure appropriate processing when data is exchanged (Taipale 2004, p. 7). By implementing rule-based processing into the software agent architecture we can create 'normative agents'. A normative agent is an agent that is able to take into account the existence of social norms in its decisions (either to follow or violate a norm) and able to react to violations of the norms by other agents (Castelfranchi *et al.* 1999). An excellent example of the use of normative agents for data mining is the ANITA project mentioned in chapter 4.

Selective revelation

The idea of selective revelation is based upon technologies and procedures that separate transactional data from identity or otherwise reveal information incrementally (Taipale 2003, p. 63). This technology is particularly useful when pattern-based inquiries are used. When pattern-based inquiries turn up information footprints that suggest deviant behaviour (e.g., a constellation of transactions that can be associated with the preparation of a terrorist attack), the identity of the person involved can be shielded from those that do not have the proper authority to view it. Only after a judge has determined that a basis exists for concluding that the pattern identified is, in fact, a pattern of potential terrorist activity and not merely a coincidental pattern of innocent activity ought the identity of the actor whose pattern is in question ought to be provided to law enforcement or intelligence officials (Rosenzweig 2003, p. 15). In this way, the use of selective revelation techniques can mitigate the possible negative effects of non-particularised searches by permitting a judicial due process between the observed behaviour and the act of revealing identity

(Taipale 2003, p. 66). It is also possible to build these techniques into agent technology itself, which further adds to the idea of normative agents.[5]

Strong credential and audit mechanisms
Transparency and accountability are essential requirements set forth by the legal framework. Through strong credential features we ensure that any possibilities for misuse and abuse are minimised. Strong audit measures ensure that possible misuse or abuse can be detected and corrected. These mechanisms must be built into the technology itself. Software agents must be equipped with tamper-proof mechanisms for reporting their actions to an appropriate oversight authority (Wahdan 2006).

9.2.3 System integration

The primary legal issue related to system integration is the fact that the integration of different surveillance systems can have effects on privacy and liberty that are not anticipated in the current legal framework. However, in this stage of the development it is difficult, if not impossible, to draft legislation that will counter possible negative effects of system integration that are caused specifically by agent-enabled surveillance. Any regulation of surveillance that is based upon distinctions in discrete technologies will become less effective in a future where systems are integrated to an increasing extent. I believe that the focus should not be on which technologies are used for surveillance, but rather on how surveillance systems impact the balance of power between the watchers and the observed when integrated. Therefore, we must place the issue of system integration in the broader perspective of the debate about electronic surveillance, privacy, and liberty. As I have described in chapter 1 technological barriers to system integration acted as *de facto* safeguards for privacy and liberty, when agents remove these barriers the legal framework must be re-evaluated in the light of this new reality.

With the advent of the ambient intelligence paradigm, we move closer to an environment where ubiquitous surveillance is not only possible, but also highly likely. In order to minimise any panoptic effects of surveillance that can result from this development, and in order to limit the power of government, I feel we must limit the room for system integration in the law. We must be particularly cautious to avoid that the surveillant assemblage, with its multitude of different surveillance infrastructures, becomes an instrument used by the government to exercise social control. While it may be justified in certain cases to use private surveillance infrastructures for the purpose of combating

5 Although selective revelation protects privacy and liberty to a certain extent, it does not provide protection against panoptic effects.

serious forms of crime and behaviour that pose a great threat to law and order (e.g., organised crime and terrorism), we must take care not to abuse liberal surveillance infrastructures for disciplinary purposes. Setting clear boundaries in the law of criminal procedure to the integration of disparate data sources is highly recommended. In particular we should limit the pro-active use of private sector surveillance infrastructures for disciplinary surveillance. While in the case of anti-terrorism it might be warranted to use private sector surveillance infrastructures pro-actively, I feel we should be extremely cautious and regularly review the use of such powers.

9.2.4 Empowering surveillance operators

Aiding surveillance operators in their tasks is one of the primary applications of agent technology. It is likely that the empowerment of surveillance operators is one of the first quantitative effects that will play a significant role in the near future.

The main question raised by this quantitative effect is how much more effective law enforcement officers and surveillance operators become as a result of using agent technology, and how we should view the authority of surveillance operators and law enforcement officers in the light of their increased effectiveness. Based on the answer to this question, we must then assess whether the legal safeguards that accompany a particular authority are still sufficient in the light of agent technology. If not, the authority of the surveillance operator or law enforcement should be revised and take into account the use of agent technology.

Possible adaptations would primarily entail removing the authority of the surveillance operator or law enforcement officer to use certain investigative powers, and limitations on the use of agent technology as described in subsection 9.1.1. Exactly how far-reaching these adaptations should be will remain subject of debate, since an answer to this question (as with most quantitative effects) is primarily of a normative, political nature and involves balancing the effectiveness of law enforcement against the protection of privacy and (individual) liberty. Moreover, it is difficult to set any clear boundaries at this point in time since the use of agent technology by surveillance operators and law enforcement agencies is still in its infancy.

One limit on the use of agent technology that should already be set at this stage is that the authority of the software agent does not exceed that of its user. For instance, if the user (a surveillance operator or law enforcement operator) is not allowed to access certain databases, the software agent should also not be allowed to access these databases.

We can judge from this section that the basis for the regulation of agent-enabled surveillance lies in the authority of law enforcement officers to use agent-enabled surveillance. Any safeguards that are to be implemented in the

legal framework will thus be dependent on the legal status of agent-enabled surveillance. Since this discussion is so closely related to the qualitative effects of agent technology (i.e., the legal status of agents), I shall discuss this topic further in subsection 9.3.1.

9.2.5 Replacing surveillance operators

From a legal point of view, the replacement of surveillance operators by agent technology altogether, is comparable to the situation where surveillance operators become more effective. Once again we must take into account the change in the effectiveness of surveillance that is caused by agent technology and consider the legal status of the agent-enabled surveillance practice in the light of this development.

It could be argued that by removing the surveillance operator from the picture we also remove his authority. If this is the case, the use of the agent-enabled surveillance method is no longer based on any explicit authority, and could thus be deemed to have no basis in the law. If this were to be the case the use of agent-enabled surveillance methods that replace surveillance operators would need to be based on an explicit authority in the law. Personally, I am in favour of this approach. In my opinion the replacement of surveillance operators by agent-enabled surveillance systems that have the ability to operate continuously can have a significant impact on privacy and liberty. Following the above reasoning would force the legislator to enact a specific statutory provision to deal with the situation. Through such a provision more specific rules can be enacted that deal with any quantitative effects the replacement of surveillance operators may have. Moreover, it seems to be in line for instance with the approach the Dutch legislator takes toward electronic surveillance technologies. In the Netherlands the use of CCTV, a technology that effectively takes away the need for patrolling, has a separate status in the law of criminal procedure.[6] One final consideration might be that by giving software agents a specific statutory basis we also provide room for more advanced applications of agent technology that could replace human operators farther in the future (i.e., undercover software agents).

Once again we see that the legal status of agent-enabled surveillance is highly relevant, therefore I shall now turn to a discussion on the legal responses to the qualitative effects of agent-enabled surveillance.

---

6 While I am in favour of a separate legal status for agent technology it is my opinion that it should be as technology independent as possible.

9.3 Dealing with the qualitative effects of agent-enabled surveillance

We have seen in the previous section that when it comes to the quantitative effects of agent technology few changes to the legal framework are actually necessary at this stage. However, when it comes to the qualitative effects of agent technology, we see a different picture. Due to the specific characteristics of agent technology changes to the legal framework need to be made in several areas. Below we discuss the legal consequences of the five qualitative effects introduced in section 7.2.

9.3.1 Legal status and qualification of investigative powers

In the discussion on the general requirements for the legal framework and the quantitative effects of agent technology we have established that the principle of legality is an important requirement when it comes to electronic surveillance, privacy, and liberty. It is my opinion that clarity on the legal status of agent-enabled surveillance is necessary in order to deal with both the quantitative and the qualitative effects of agent technology.

There are several different options when it comes to providing software agents with a legal status. The most likely options are: (1) viewing software agents merely as tools used by law enforcement officers, (2) vesting authority in software agents through their users, (3) codifying the use of software agents as a specific investigative power, or (4) defining software agents as separate entities in the law of criminal procedure.

The first option is to regard software agents merely as tools used by law enforcement officers. When we view software agents as tools that aid law enforcement officers in the exercise of their duties, there is no need to give them a specific legal status and thus no need to further codify their use in the law of criminal procedure. In this case their application would be covered by the existing rules of criminal procedure. In my opinion this option would only be sufficient for applications of agent technology that do not pose a serious threat to privacy and liberty. This is primarily the case when agent technology would be used to support certain police tasks, such as the allocation of extra police resources to a certain area that (agent-enabled) data mining has revealed to be a high-risk area.[7] However, as I discussed in subsection 8.3.5, we should be careful when it comes to considering agent technology merely as tool for law enforcement officers in the case of more privacy-sensitive applications and liberty-sensitive applications. The increased effectiveness of

7 The Police of Amsterdam for instance uses a data-mining suite known as 'DataDetective' that can facilitate this type of intelligence led policing. See for more information: <http://www.sentient.nl>

agent-enabled surveillance may affect privacy and liberty to such an extent that a legal structure is necessary which can provide a greater degree of control and accountability. Moreover, when law enforcement officers use advanced software agents that display high levels of autonomy and intelligence (i.e., agents with a strong notion of agency), it could well be that the software agent's capabilities enable it to execute certain investigative actions autonomously that exceed the authority bestowed upon the law enforcement officer himself. It would then be necessary to determine after the fact whether the law enforcement officer was actually allowed to use the agent as an investigative tool. This problem could be avoided by linking the authority of the user to that of the agent, which brings us to the second option.

The second option is to vest authority in the agent through the law enforcement officer that uses it. While in the context of criminal law the question on how to vest authority in an agent is rather new, a similar debate has been going on for some time in the context of private law. An approach that has been proposed in the context of private law is to address this issue via the law of agency. Agency is the *relationship* between the principal and the agent, based on *authority*, or the power conferred on the agent to constitute legal relations between the principal and a third party (De Miglio *et al.* 2002). While in a commercial setting the law of agency might be well suited, a law enforcement officer cannot normally confer his rights and duties to a third party unless there is a specific statutory provision (Schafer, Rodriguez-Rico, Vandenberghe 2004, p. 156). Especially in those cases where software agents have a high level of autonomy a clear statutory basis must be provided. This is necessary in order to bring the use of agent technology for surveillance and investigative purposes in line with the requirements of article 8 ECHR (most importantly, that the use of agent technology must be in accordance with the law). So, if we are to provide a legal status to software agents through the law of agency, a specific statutory provision will be necessary. Such a provision could state that the authority to use the agent is based on the authority of its user. Any investigative powers that would be used by the agent would then reach as far as those of the law enforcement officer that deploys it. While this approach would meet the requirement of legality, it will most likely also contribute to the situation described in subsection 8.3.5, namely that through agent technology law enforcement officers will become more adept at executing their tasks than anticipated by the legislation that governs their authority. So, when we regulate the use of agent technology in this way we run the risk that the legal framework will provide inadequate safeguards. Therefore, this approach to giving software agent a legal status is only feasible in those cases where the impact on privacy and liberty is small or at most limited.

The third option is to codify the use of software agents as a distinct investigative power in the law of criminal procedure. This option is of particular interest in those situations where the impact of agent-enabled surveillance on privacy and liberty is high. An example of this could be the pro-active investi-

gation of criminal offences. By codifying the use of software agents explicitly in the law of criminal procedure we can address the quantitative and qualitative effects of agent-enabled surveillance more effectively as well as enhance the foreseeability of agent-enabled surveillance. Codifying the use of agent technology as a separate investigative power in the law of criminal procedure is only relevant in those cases where the specific characteristics of agent technology (most notably autonomy, emergent behaviour, and adaptability) are actually determining factors in the use of the investigative method. When agent technology is an integral part of a broader investigative technique such as data mining, there is no need to codify its use as a specific investigative power. A possible drawback of codifying the use of agent technology as a separate investigative power, however, is that it runs the risk of being technology dependent. Therefore, in formulating the use of agent technology as an investigative power we must take care not to focus too much on the current technology. Rather, a distinct investigative power should focus on those attributes of software agents that are relevant when it comes to privacy and liberty, *viz.* autonomy, emergent behaviour, and adaptability. This option is therefore most relevant when software agents or agent systems display higher levels of autonomy, adaptability, and possibly emergent behaviour.

The fourth option is to consider software agents as separate entities within the process of law enforcement altogether. In the context of private law and legal philosophy the idea has been forwarded to grant legal personhood to artificial intelligences such as software agents (see, for instance: Solum 1992). This notion brings up legal questions about how to confer rights and duties to an agent, and philosophical questions on what exactly constitutes personality and identity. In my opinion these questions are still part of a largely theoretical debate, which is only relevant when strong artificial intelligence becomes a reality. However, by giving agents a separate status within the law of criminal procedure (without necessarily granting them legal personhood) we do acknowledge their unique characteristics and the qualitative effects they may have. A separate status for software agents in the law of criminal procedure would also provide a basis for the more permanent use of software agents. When software agents are characterised as (special) investigative power, their use must be warranted on a case-to-case basis. As we have seen in the previous chapters one of the strong points of agent technology is their ability to be active for an indefinite period of time. A separate status within the law of criminal procedure (comparable to that of a police officer, a detective, chief detective, *et cetera*) would allow for the permanent use of software agents, based on authorities described in the law. Looking more towards the future, this kind of legal status for software agents also opens up the way for agents to conduct undercover activities and other tasks that require strong artificial intelligence.

9.3.2 Jurisdiction

The current legal framework sets forth the rules that law enforcement agencies have to abide by when they wish to obtain information located in a different jurisdiction. When software agents take over the tasks exercised by law enforcement officers, they have to abide by the same rules. While the topic of jurisdiction has many facets, only the topic of mutual legal assistance in criminal investigations is relevant for the subject matter of this thesis.

In order to combat international crime and terrorism countries establish treaties (either bilateral or multilateral) that enable mutual legal assistance in criminal investigations. Especially the threat of international terrorism has led to greater cooperation between nations in the area of criminal investigations. It is outside the scope of this thesis to explain the rules for mutual legal assistance in both the Netherlands and the United States fully. What is important to note in the context of this thesis is that mutual legal assistance also covers the gathering and the exchange of (personal) data by law enforcement agencies.

When it comes to the legal issues surrounding the processing of data by software agents in an international context we must distinguish among three different situations. The first situation relates to software agents gathering publicly available (personal) data from the internet. The second situation relates to software agents from one nationality gathering data from databases and agent platforms that fall under a different jurisdiction. The third situation relates to the exchange of data between law enforcement agencies of different nationalities.

Since the internet is a public place, investigators can conduct investigations aimed at persons with a different nationality more or less freely on the internet, without a specific need for mutual legal assistance. Article 32 of the Cybercrime Convention (to which both the Netherlands and the United States are party) covers this situation. Parties in the Cybercrime Convention may:

> "a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
> b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

In the second and third situation the normal rules of mutual legal assistance (also covered by the Cybercrime Convention) apply. While further research is needed in this area, it is my opinion that at this stage no specific rules need to be enacted that deal with the qualitative effects of agent technology on the legal framework for mutual legal assistance. The qualitative effects of agent technology can be addressed by implementing the existing rules in the technology. Once again proper identification, authentication, and authorisation

mechanisms are vital when it comes to effectuating existing rules for mutual legal assistance. Apart from these mechanisms, an additional demand in the area of mutual legal assistance is that the nationality of the agent must be identifiable. As such the legal status of the agent, and the authority on which its use is based must be sufficiently clear.

9.3.3 Transparency and accountability

Issues that are likely to emerge when software agents are used for law enforcement purposes are a potential lack of transparency and difficulties with regards to accountability. These important issues must be addressed in the legal framework and effectuated through technological and procedural measures.

Transparency
Transparency is of particular importance in the context of agent-enabled surveillance since software agents are often 'black boxes'. What I mean by this is that it is oftentimes unclear how an agent has attained its goals. In general the fact that agents tend to be black boxes is not a problem, but part and parcel of the agent philosophy. Since the design goal of a software agent is to fulfil a task specified by the user, it is logical that it only delivers the desired result and does not explain the whole range of actions that it performed leading up to the desired result. However, in the case of law enforcement it is essential to keep a close watch on the actions of a software agent from the viewpoint of transparency (and accountability). It is to be expected that advanced software agents will make decisions autonomously that could affect privacy and liberty (for instance decisions on whether to query certain databases). When it comes to the transparency of agent-enabled surveillance systems two questions are particularly relevant: (1) how does the agent reach a particular decision? and (2) on what information has the agent based this decision?

A software agent makes decisions based on input that is processed by its internal reasoning system. While it is not necessary to state explicitly how the reasoning process works, decision-making should not be a total black box in order to increase legal certainty. Mechanisms must therefore be in place that can help clarify the decisions taken by the internal reasoning system *ex post*. Logging is of particular relevance when it comes to clarifying the behaviour of software agents.

The internal reasoning system of an agent can only make decisions based on input from its environment. So, knowledge about the source and the quality of the input are vital when it comes ensuring the transparency of decisions made by the software agent. This subject is closely related to that of use limitation (see subsection 9.3.4). Transparency is less of a problem when it is clear what types of data a software agent may process and what the sources are where the agent may gather these data.

A second significant aspect when it comes to transparency is the quality of the law that governs the application of agent-enabled surveillance. In this area the requirement of foreseeability is particularly relevant. The requirement of foreseeability states that the law must be sufficiently clear in its terms to give an adequate indication of the circumstances in which and the conditions on which public authorities are empowered to resort to a given investigative power. However, in the case of advanced software agent applications, the investigative method on which the investigative power is based itself has the ability to adapt and change, making it less clear what the actual investigative power entails. Here we see a tension between the 'flexibility' of advanced software agent applications and the need for the law to be precise. It is vital that a balance is struck between these two aspects in the legal framework.

Accountability
Next to providing transparency an important task is to ensure the accountability of agent-enabled surveillance. Since the potential impact of agent-enabled surveillance and law enforcement on privacy and liberty is high, we must take care to ensure that proper mechanisms (both of a technological and a procedural nature) are in place to ensure the accountability of agent-enabled surveillance. The legal framework should make these mechanisms mandatory. Since accountability is already a legal requirement when it comes to electronic surveillance, it is not necessary to state explicitly that agent-enabled surveillance must be accountable. Rather, this general requirement should be tailored specifically to agent-enabled surveillance in additional guidelines, such as the *Aanwijzing voor de Opsporing* (Guidelines for Investigations) in the Netherlands or the *Attorney General's Guidelines* in the United States. When it comes to ensuring accountability one technological measure that must be implemented is proper logging mechanisms. Software agents and agent systems can also be equipped with a logging subroutine. Based on the log that an agent keeps of his actions we can determine (in retrospect) what the agent has done, and on what information it based its decisions.

9.3.4 Use limitation

It is likely that threats to privacy and liberty will be greater when software agents display high levels of autonomy and the authority vested in them is substantial. Therefore, it is necessary to limit the use of advanced software agent applications in certain instances. In my opinion, the general requirements in the area of use limitation as discussed in subsection 9.1.1, which apply to both the quantitative and qualitative effects of agent technology, should be accompanied by specific rules on use limitation tailored to the specific characteristics of agent technology. However, drafting these rules could turn out

to be a daunting task, something that is primarily related to specific characteristics such as emergent behaviour and adaptability.

Emergent behaviour

Emergent behaviour is an important issue that must be dealt with in the legal framework. In multi-agent systems emergent behaviour might lead to unexpected situations not foreseen in the legal framework. It is evident that in order to ensure legal certainty the foreseeability of agent-enabled surveillance must be guaranteed. In order to safeguard privacy and liberty any uncertainty that flows forth from the complexity of multi-agent systems must be kept to a minimum. This then can lead us to no other conclusion than that the use of agent-enabled surveillance applications that could give rise to emergent behaviour should be either prohibited or at least kept to a minimum.

There are several options to limit emergent behaviour and any negative effects that might result from it. I shall mention four of them. A first option is to include a specific restriction in the legal framework on the use of advanced agents systems likely to give rise to emergent behaviour. A second possibility is to only warrant their use in those cases where there is a serious threat to law and order. A third option is to limit the use of these kinds of systems to the intelligence community and not allow the use of multi-agent systems that can give rise to emergent behaviour in criminal investigations. If lawmakers and policymakers do decide to use such systems, a fourth option would be to exclude those pieces of information that are the result of emergent behaviour as evidence.

Adaptability

When it comes to defining and limiting the investigative powers of software agents, a particular issue is raised by software agent adaptability. When we look at the current breed of surveillance technologies we can establish that they do not have the power to adapt. Consequently, the impact of investigative methods can be established more or less clearly and rules regarding their use drafted accordingly. However, when an investigative method can change and improve itself, the task of drafting rules for its use becomes less straightforward. This raises serious questions such as: (1) what is the authority given to an autonomous agent capable of learning new skills? (2) how do we define their use as an investigative method? and (3) what limits should be placed on the adaptive abilities of software agents? In the current legal framework (both in the Netherlands and the United States) we find no answers to these questions.

The first step in defining and limiting the surveillance power of software agents that have the ability to adapt is clarifying their legal status. When it comes to more advanced software-agent applications, such as those that have the capability to adapt, I think they can no longer be viewed merely as simple tools that aid law enforcement officers. Rather, their use should be based either

on the authority of the user, or a specific provision in the law of criminal procedure. In this way we can ensure that the necessary rules and proper safeguards are implemented.

The second step is to define the rules for the use of advanced agents. It must be noted that we must allow some room for autonomy and adaptability. Since 'real' law enforcement officers also become more efficient and effective over time due to their experience, it is logical to allow some room for adaptation in advanced software-agent applications. However, it is likely that the pace at which adaptable agents will learn is much faster than that of real law enforcement officers. Therefore, boundaries need to be set in the legal framework. What these boundaries are and how strict the rules for the use of advanced software agents must be set, will depend on the actual surveillance application. For this we can follow the rules set forth by the current legal framework and view it in light of the increased accessibility of information and the adaptability of software agents. If it turns out that the rules set forth in the current legal framework are inadequate we can limit the use of adaptable agents by implementing some of the ideas on use limitation set forth in subsection 9.1.1. With regard to setting rules for agent-enabled surveillance it is particularly relevant to ensure that the boundaries set in the law and the accompanying procedural safeguards (e.g., obtaining a warrant, or notifying a suspect) remain adequate when the agent application becomes more powerful over time. So when a software agent evolves over time, the procedural safeguards should evolve along with the agent itself. It will be a challenge for the legislator to build a legal framework that is flexible enough to deal with advanced software-agent applications. It seems likely that in the future periodic reviews of software-agent applications will be necessary to ensure that the law that governs their use is still adequate. However, a different approach could also be taken. In order to curb the negative consequences a rule could be set that states that an adaptable agent does not have the authority to access data sources not specified in the warrant on which its use is based. Implementing this rule would effectively negate any negative consequences of software-agent adaptability. However, it would also mean that any benefits law enforcement could have from using this technology would be negated as well.

The third step is to effectuate the rules for the use of advanced software-agent applications through technology. The rules set forth in the legal framework must be translated to clear parameters for the operation of software agents. In this area the processing of (personal) data by software agents is of particular relevance. Therefore, the idea of normative agents that know which data they may process under which circumstances is once again important.

9.3.5 Strength of the agent metaphor

While the strength of the agent metaphor might trigger panoptic effects, it is difficult to counter this development by means of regulation. The reason is that any panoptic effects that will occur due to the strength of the agent metaphor are triggered by psychological and sociological reactions to the extensive use of agent-enabled surveillance. These reactions flow forth from a complex set of events and cannot be attributed to a single event that can be prohibited or otherwise regulated.

It is my opinion that awareness about the role of agent-enabled surveillance in society is the best way to counter any negative effects that the strength of the agent metaphor may have. When lawmakers, policymakers, and individuals understand the power and potential of agent-enabled surveillance there is a solid basis for a discussion about the positive and negative effects of agent-enabled surveillance, and measures can be taken to avoid a situation that could give rise to panoptic effects. One such measure, for instance, would be to limit the widespread use of agent-enabled surveillance.

9.4 Towards a legal framework for agent-enabled surveillance

In section 2.8 described a possible timeline for the development of agent technology. From this timeline we may judge that the development of agent technology for surveillance purposes is still in its infancy. But given the fact that technology changes at a rapid pace and the legislative process in general is unresponsive to these changes, awareness about the possible effects of agent technology on the legal framework is required in an early stage. While I feel awareness is important, it is counterproductive to change the legal framework in this early stage to accommodate for technology that is not yet in existence. Rather, changes to the legal framework should closely follow the projected growth path of agent technology.

Judging from the legal issues related to quantitative and qualitative effects of agent technology, and the possible solutions thereto, I feel it is wisest to pursue a twofold strategy when it comes to dealing with agent technology in the (near) future. The first part of the strategy is dealing with the quantitative effects of agent technology by rethinking the law for electronic surveillance and privacy. The second part of the strategy is gradually adapting the law over time to new technological realities, such as advanced agents with a strong notion of agency. It is my opinion that following this twofold strategy we can guarantee that the legal framework can keep fulfilling the functions set forth by Van Hoecke (2002).

9.4.1 Quantitative effects: rethinking privacy?

In its relatively short life as an explicit right, privacy has undergone many transformations, mainly in response to technological changes. At the threshold of the ambient-intelligence paradigm it seems that privacy is set for yet another facelift. Since the quantitative effects of agent technology make up only part of the changes brought about by the ambient-intelligence paradigm, we must place them in the broader context of a discussion about electronic surveillance and the law. In this discussion the changing role of privacy and the difficulties of balancing privacy against security are most relevant. Moreover, we have seen that there are no easy legislative solutions in the area of quantitative effects that solve the problems posed by the surveillance sorites paradox and the slippery slope of electronic surveillance. Therefore, I shall discuss the road towards an enhanced legal framework in the light of this broader discussion.

Is privacy really the issue?
Central to the debate about surveillance, privacy, and liberty is the question how the privacy interests of individuals should be balanced against the interest of society in greater security. On the one side, privacy advocates argue that privacy is an inalienable right and infringements of privacy made possible by surveillance technology must be avoided at almost any cost. On the other side of the debate, we see law enforcement and the intelligence community pushing for more investigative powers with the aim of combating organised crime and terrorism more effectively. As a value privacy is thus continuously in conflict with other interests in society such as (national) security. It seems that in the age of international terrorism a higher value is placed on security, and only a few people object to the loss of privacy incurred in the process, especially given that the negative effects of a significant loss of privacy become apparent when the damage is already done. These negative effects however, are not the loss of privacy in itself, but rather the loss of liberty, discrimination of groups and individuals, and the collapse of social cohesion.

In those areas where the government encroaches upon liberty (most notably negative liberty), we see that the right to privacy is oftentimes used to defend against an infringement. There are a number of cases, especially in the jurisprudence of the United States Supreme Court, that illustrate this point. A clear example is the case of *Griswold v. Connecticut*.[8] In this case the Supreme Court constructed a conception of privacy out of reproductive rights (Bailey 2004, p. 174). In a sense, privacy is thus a derivative right used to protect the higher interest (in this case reproductive rights) on which its application is based. However, that we do not always need to invoke the right to privacy in order to curb the negative effects of electronic surveillance can also be seen in a

8 United States Supreme Court, *Griswold v. Connecticut*, 381 US 479 (1965).

number of cases brought before the Supreme Court. Though the Court has at times used the right to privacy to protect First Amendment interests (see, for instance, the case of *NAACP v. Alabama*), we see that this is by no means necessary (Blok 2002, p. 157).[9] In the case of *Talley vs. California* it was ruled that a prohibition to distribute political flyers anonymously was a violation of the freedom of speech. The ruling did not include any reference to the right to privacy (Blok 2002, p. 157).[10] Other examples include *Shelton v. Tucker* and *Sweezy v. New Hampshire*.[11] By acknowledging the fact that the right to privacy is oftentimes merely a means to protect a higher interest, we avoid a large amount of confusion. But more importantly, cases that deal with surveillance and individual liberty can be judged on the basis of their own merits and do not have to rely on the right to privacy that has become so difficult to define and uphold in the information society.

Surveillance ultimately remains a means of exercising control and as an instrument of power it is therefore almost by definition susceptible to misuse and abuse. Any discussion about the possible negative effects of surveillance must therefore concern itself with the real issues at hand: limitations of liberty, possibilities for discrimination, and the collapse of social cohesion. Moreover, a preoccupation with the conception of privacy as limit to power leads to a disregard of the other conceptions of privacy pivotal to the well being of the individual and the functioning of society. By acknowledging that privacy as limit to power is a means to a greater good, *viz.* liberty, equal rights, and social cohesion, we open up room for the full spectrum of human rights in the discussion about surveillance and its effects on the individual and society. An added benefit of this approach is that it also allows the other conceptions of privacy that have been overshadowed by the conception of privacy as limit to power, to gain more attention.

Is privacy really the answer?

We have seen that the debate about privacy is currently focussed on maintaining privacy in order to limit the power of government. More recently a third voice can be heard in the debate, one that argues for greater transparency instead of privacy. Its main protagonists, Brin (1999) and Bailey (2004) both argue that the secrecy paradigm that is central in the debate about privacy, liberty, and surveillance is neither desirable nor feasible in the information society. They argue that since information wants to be free and we are moving towards a world where technology makes gathering and processing (personal) data increasingly simple, trying to maintain privacy is a lost cause. Instead they argue that we should embrace the idea of transparency in favour of

9 United States Supreme Court, *NAACP v. Alabama*, 357 US 449, 462 (1958).

10 United States Supreme Court, *Talley v. California*, 362 US 60 (1960).

11 United States Supreme Court, *Shelton v. Tucker*, 364 US 479 (1960); United States Supreme Court, *Sweezy v. New Hampshire,* 354 US 234 (1957).

privacy. It is their idea that only through complete openness we can discover individuals that pose a threat to our society. However, asymmetries in transparency shift the balance of power towards those who have most information and disclose least. Therefore, mechanisms such as synoptic surveillance, as right to participation, and some form of reciprocal transparency are necessary (see section 3.7).

While I feel both Brin (1999) and Bailey (2004) disregard the importance of privacy and place too much trust in the idea of reciprocal transparency (which is a fiction in my opinion), they do make an important contribution to the discussion about privacy and liberty. Their assertion that the right to privacy is not necessarily the best barrier against invasions of liberty provides an interesting alternative argument in the 'privacy versus security' debate. In particular their argument that privacy is unresponsive to life in the information society is sound. Before the advent of electronic surveillance technology, privacy was an inherent part of our physical reality. However, due to the rapid pace of technological development, the link with the physical world is becoming increasingly less clear. While the right to privacy has been updated numerous times over the course of its existence to accommodate for these changes, it still struggles to keep up. This is the main cause of the problems mentioned in section 6.4 that contribute to the inability of privacy to provide an adequate answer to the societal issues surrounding electronic surveillance.

If we conclude that the right to privacy cannot provide full protection of (individual) liberty in the light of electronic surveillance, we are left with two alternatives: (1) to redefine the right to privacy in order to bring it in line with the technological reality, or (2) to look for alternative mechanisms for the protection of individual liberty that can work alongside the right to privacy.

The future of surveillance and privacy

As I described throughout this thesis, the right to privacy (in its current incarnation) is inadequate for the full protection of privacy and individual liberty. It goes without saying that this does not mean that we should disregard the existing framework for the protection of privacy and individual liberty altogether, since the right to privacy still plays an important rule in maintaining both privacy and liberty. In particular, data protection principles are of significant importance. However, I do not believe that it is right to continue to view the right to privacy as the primary barrier against infringements of liberty. Therefore, I feel we must not redefine the right to privacy yet again to accommodate for the technological changes that are occurring around us. In my opinion a new definition of the right privacy will face the same difficulties as the current incarnation of the right to privacy, without providing substantial benefits for the protection of liberty.

When we examine the current conceptions of privacy in the light of the subject matter of this thesis we may establish that the most relevant conception of privacy is that of a means to limit power. In this sense the function of the

legal framework for privacy is to create a sphere of autonomy for the individual. Privacy is one way creating a sphere of autonomy. However, it is by no means the only one. We should make a better assessment whether the actual purpose of the legislation should be the protection of privacy, or the protection of liberty. In other words: is privacy a means or is privacy a goal? Far too often privacy is merely the means by which (individual) liberty can be protected, but not the goal in itself. It is possible that better legal mechanisms are available, such as protection through the freedom of speech, the right to association, or the right to equal treatment under the law.

In chapter 5 we established that the right to privacy is firmly rooted in the tradition of negative liberty. Up until now this approach provided us with an adequate amount of protection of privacy and liberty. However, we are gradually reaching a point in time where the power of electronic surveillance is becoming so strong that it can facilitate social control and has the power to influence people to a significant degree. Here then we enter the realm of positive liberty where we must ask ourselves the following question: does the advent of electronic surveillance influence the ability for people to take informed decisions for themselves about what is right in life? Electronic surveillance can influence the positive liberty of individuals in two ways: (1) it can cause panoptic effects that inhibit individuals in their liberty, and (2) the power of surveillance can be used to exclude, to influence, and even to manipulate people. So, if there is proper cause to assume that electronic surveillance will influence the positive liberty of individuals or groups, we should be very careful in using such a technology.

As we move towards the ambient-intelligence paradigm we will see greater pressure from electronic surveillance on positive liberty. Following the reasoning of Brin (1999) and Bailey (2004) we arrive at the conclusion that privacy cannot provide adequate protection for positive liberty in the future by itself. Therefore, in the future we should look for protection mechanisms to function alongside the right to privacy. Taking the general considerations of section 9.1 into account it is my opinion that four protection mechanisms deserve considerable additional attention in the discussion about surveillance, privacy, and liberty.

A first mechanism to ensure liberty is a heightened awareness about surveillance technology and its possible effects. In raising awareness we should not focus on the effects electronic surveillance may have on privacy, but rather on the societal impact of electronic surveillance. In particular, we should examine the possible panoptic effects of surveillance and determine how surveillance influences positive liberty. Furthermore, we should examine whether surveillance is aimed disproportionately at certain groups and how this affects social cohesion within our society.

A second mechanism is to give more attention to human rights and civil liberties that up until now relied too much on the right to privacy for their protection. Of particular relevance in this context is how information is used

and how this influences the liberty of individuals as well as groups. Therefore, it is my opinion that there should be less focus on privacy and the rules surrounding personal data, and more focus on 'constellations' of data and the use thereof. It is no longer realistic to judge the use of data according to the outdated standards of privacy, which have their basis in a technological reality that no longer exists. As we move towards the ambient-intelligence paradigm we should place less faith in concepts such as the 'reasonable expectation of privacy criterion' in favour of concepts that pay more attention to the reality of advanced electronic surveillance. Therefore, I would like to recommend a 'surveillance impact criterion' in judging whether the application of a surveillance method is legitimate. Such a criterion would entail that a judge not only establishes whether there has been an invasion of privacy (along the lines of article 8 ECHR, or the jurisprudence of the Supreme Court), but also how the use of the information gathered over the course of the surveillance exercise impacts the individual.[12] While difficult to implement, it would be particularly valuable that an examining magistrate would review the impact of surveillance *ex ante*. Furthermore, this criterion could be used to establish what the impact of surveillance and monitoring is on groups (especially ethnic or religious minorities).

A third mechanism of ensuring liberty is the implementation of existing rules and legislation in surveillance architectures and infrastructures through code. In order to curb the power of electronic surveillance, barriers must be erected by the technology itself. Since technology by itself is neutral, mechanisms such as normative agents are vital when it comes to ensuring privacy, but more importantly, liberty.

A fourth mechanism of ensuring liberty is guaranteeing that individuals have the means to effectuate their right to participation. While it is my opinion that full reciprocal transparency is a fiction, greater transparency will help to balance the power between the watchers and the observed. Moreover, it will provide additional means to ensure the accountability of government surveillance. Interestingly, one of the best tools for citizens to effectuate their right to participation is agent technology. Historically, surveillance has been the province of the state, since surveillance in general is cost and labour intensive. Through software agents we can place surveillance power in the hands of citizens, giving them the means for synoptic surveillance.[13]

It is questionable whether the measures and mechanisms proposed above would require specific changes to the law. In my opinion such changes should

12 The Dutch Data Protection Act already establishes that certain types of personal data are considered 'sensitive'. This includes data regarding ethnicity, religion, sexuality, and political affiliation.

13 In those cases where covert surveillance (for instance wiretapping) has been authorised, an exception must be made to ensure that suspects are not able to establish whether they are being monitored.

only be made if it is necessary to deal with the specific characteristics of agent technology. Which brings us to a discussion about the future of the legal framework in light of the qualitative effects of agent technology.

9.4.2 Qualitative effects: implementing new rules for a new technology

In my opinion the continued development of agent technology will eventually force the legislator to adapt the legal framework to accommodate for the specific characteristics of agent technology. In particular, the ability of software agents to act autonomously, adapt, and react to changes in their environment forms a break with past surveillance technologies. Furthermore, the likelihood of emergent behaviour in complex multi-agent systems also needs to be addressed. We have established that when it comes to the qualitative effects of agent technology it is particularly relevant to ensure that agents have the proper authority to conduct surveillance. Based on the proper authority, we can implement the specific legal safeguards described in this chapter. The four main options that exist in this area (i.e., considering agents as tools, granting them authority through the user, considering agents as a special investigative power, and giving them a separate legal status) can be used to regulate the use of agents along the growth path established in section 2.8.

In the first phase of software-agent development (that of closed agent systems), the use of agent technology will not yet require a specific legal basis. In this phase the agents used for law enforcement purposes are still pretty simple and therefore it is unlikely that they will cause any qualitative effects. In this phase, it is probably sufficient to consider agents merely as tools for law enforcement, or base the authority for the use of software agents on that of the user. Given the limited trust that is placed in the use of agent technology at this stage and the general lack of speed in the legislative process, it is my estimate that this phase will last roughly from 2006 until 2010.

In the second phase (that of cross boundary systems) it is more likely that qualitative effects will manifest themselves. In particular qualitative effects related to the integration of distributed data sources, such as, jurisdiction, transparency and accountability, and use limitation, are likely to emerge. It is therefore important to start thinking about the legal framework before this phase actually becomes a reality. It does not seem likely that in this phase of agent development advanced software agents that feature high levels of autonomy and adaptability will be used for law enforcement purposes. But when they do, appropriate measures should be taken. It is my estimate that the second phase of the legislative process will start around 2010 and will last up until 2015.

In the third phase (that of open systems) software agents will be able to communicate with a vast number of heterogeneous and distributed data sources due to improved interoperability of systems and their ability to adapt.

Issues such as, jurisdiction, transparency and accountability, and use limitation, will become significant in this phase and must be dealt with in the legal framework. Since agents will become very powerful surveillance tools in this phase, I feel it necessary to qualify their use as a specific investigative power in the law of criminal procedure. Moreover, due to advances in AI research it is also likely that in this phase of software-agent development advanced software agents will be employed by law enforcement. If this is the case, appropriate safeguards in the legal framework, effectuated through technology and procedures, must be put in place. This phase of the development of the legal framework for agent-enabled surveillance will last from 2015 up until to 2020.

In the fourth phase of agent-development (that of fully scalable systems) agents will display all of the specific characteristics that can give rise to qualitative effects. Therefore, I feel that in this phase agents should be granted a separate status in the law of criminal procedure in order to guarantee the highest level of legal certainty. It is my estimate that this phase of the legislative process will last roughly from 2020 to 2030.

When we compare the development of agent technology in general to that of the legislative framework, we see that the legal framework will probably lag behind the technological developments. While this situation is by no means unique (in general, the law lags behind technological developments), I feel we must ensure that the legal framework for the regulation of agent-enabled surveillance is adequately suited to the state of the technology, in order to minimise any possible negative effects of agent-enabled surveillance.

9.5 PROVISIONAL CONCLUSIONS

In this chapter we examined possible solutions to the legal issues that surround the use of agent technology for law enforcement purposes. We may say that the impact of agent technology on surveillance and law enforcement is potentially substantial, something that needs to be reflected in the thinking about the legal framework for surveillance, privacy, and liberty.

We have established that it is particularly difficult to deal with the quantitative effects of agent technology. There are no clear legislative solutions that can be implemented which would address the quantitative effects of agent technology in a comprehensive manner. Rather we must view the use of agent technology in the broader picture of electronic surveillance and society. Increases in surveillance tend to send us further down the slippery slope. Therefore, we must be vigilant when it comes to the use of agent-enabled surveillance. Awareness about the possible effects of agent-enabled surveillance is crucial in the discussion about surveillance, privacy, and liberty. In this discussion, it is also crucial that we acknowledge that the right to privacy is not the only bulwark in the protection of liberty.

When it comes to dealing with the qualitative effects of agent technology we see that they must be addressed through changes in the existing legal framework. In both the law of the Netherlands and the United States, there is no clear legal status for software agents, which is a necessary first step to address the qualitative effects of agent technology. By giving software agents a clear status in the law of criminal procedure, we increase legal certainty and provide a solid basis from which to address the distinct qualitative effects of agent technology. In my opinion, legal issues stemming from specific characteristics such as autonomy, emergent behaviour, and adaptability, deserve specific mention in the legal framework for agent-enabled surveillance.

In addressing the legal issues surrounding the use of agent technology we should not disregard the significance of technological and procedural measures. While the general rules are set forth in the legal framework, these rules must be effectuated in the technology itself and the accompanying procedures. In this area the work that will be performed on normative agents is particularly relevant.

10 Conclusions

Quis custodiet ipsos custodes?
Decimus Iunius Iuvenalis

In this thesis I investigated the use of agent technology for surveillance purposes and assessed how the use of agent technology would influence the legal framework for the protection of privacy and liberty. Over the course of this thesis I have tried to bring together insights from various fields of science, most notably law, sociology, and computer science, and apply them to the issue of software agents, surveillance, and privacy. In this final chapter I shall answer the problem definition and the research questions posed at the beginning of this thesis and draw my final conclusions.

In section 10.1 I shall give a recapitulation of the current technological and cultural developments in our society that give rise to the problem definition of this thesis. In section 10.2 I shall discuss agent-enabled surveillance and answer the first research question. In section 10.3 I shall describe the impact of agent-enabled surveillance on privacy and liberty and answer the second research question. In section 10.4 I shall draw my conclusions on how the legal framework for privacy and liberty is influenced by agent-enabled surveillance and describe why I feel it must be changed. This answers the third research question. In 10.5 I shall summarise the most important measures and mechanisms that can contribute to a better legal framework for the protection of privacy and liberty. This answers the fourth research question. Then, in section 10.6, I shall draw my final conclusions in relation to the problem definition. I shall end this thesis by giving some suggestions on future research in section 10.7.

10.1 The essence of surveillance technology

As described in chapter 6 the birth of modern science took place during the Enlightenment. As a result, belief in a supernatural entity that governs our lives gradually gave way to a scientific approach to live. The primary goal of science is to create useful models of reality through which we can gain a greater understanding of our environment. We can use this knowledge to exercise control over our environment by means of technology. Therefore, knowledge is power. While science is concerned with acquiring knowledge,

technology is concerned with the actual application of knowledge for a particular purpose. According to Mumford (1934, p. 10) "the attempt to modify the environment in such a way as to fortify and sustain the human organism" is the essence of technology. Over the course of history man has developed increasingly effective ways of modifying and controlling his surroundings. The creation of tools with which to manipulate the environment was the first step in the evolution in technology.[1] A second significant step in the evolution of technology was the creation of machines. According to Mumford (1934, p. 10) the essential distinction between a tool and a machine "lies in the degree of independence in the operation from the skill and the motive power of the operator: the tool lends itself to manipulation, the machine to automatic action". In my opinion the advent of artificial intelligence marks a third important step in the evolution of technology. Since artificial-intelligence machines (i.e., robots and software agents) became capable of thought and autonomous action. The indirect management made possible by artificial intelligence enables a greater degree of control, something that flows forth from the interaction between the physical world and cyberspace.

The notion of cyberspace as a virtual information space existing alongside the physical world plays an important role in the context of this thesis. We have established that we are gradually moving towards the 'ambient-intelligence paradigm'. The arrival of this new computing-paradigm is the result of advances in information and communication technology, which can be contributed to a growing demand for efficiency, speed, convenience, and risk-management in the information society. Whereas in the personal computer paradigm cyberspace was largely separated from the physical world, in the ambient-intelligence paradigm the physical world and cyberspace are deeply integrated. As we move through the physical space and interact with it (for instance by making transactions), our movements and actions will be captured and recorded in cyberspace. What this means is that a greater degree of control cannot only be obtained in cyberspace, but that this control also extends to the physical world. At the time of writing this thesis we are in the early stages of the ambient-intelligence paradigm. Already huge amounts of data are created and processed on a daily basis within the surveillant assemblage and this volume will increase exponentially over the years to come as we move closer to the realisation of the ambient-intelligence vision.

We thus may conclude that electronic surveillance, which depends on the processing of (personal) data for its effectiveness, will become even more powerful in the coming years. In particular the relation between actions performed in the physical world and the records of those actions kept in cyberspace will contribute much to the effectiveness of surveillance and control.

---

1 There are many different ways to describe the history of technology. I base my short description on the effectiveness of the means with which mankind influences and modifies his environment and exercises control over his surroundings.

As I have argued throughout this thesis, more effective surveillance will shift the balance of power between the observers and the observed in favour of the observers. However, we have also established that the problem of the information overload hampers the effective exercise of surveillance and control. The sheer volume of data makes distilling appropriate information and knowledge a difficult task. Because the problem of information overload is becoming increasingly prevalent in the information society, indirect methods of exercising control are becoming increasingly important. Software agents, either by themselves or used in conjunction with other artificial-intelligence tools, are an essential means in overcoming the information overload.

10.2 THE ESSENCE OF AGENT-ENABLED SURVEILLANCE

The first of the research questions to be answered was formulated as follows: *How will agent technology influence surveillance practice?*

In chapter 4 we established that the primary applications of agent technology for surveillance purposes are (1) mediation services and query brokering, (2) the augmentation of human operators, and (3) the replacement of human operators altogether. In general, this will influence surveillance in the sense that many surveillance tasks will be automated and as a result thereof become more efficient and effective. Moreover, the scope and duration of surveillance can be expanded since no significant extra costs (i.e., the cost of manpower) will be incurred by expanding surveillance.

In the short-term future software agents will be used to provide all of the above-mentioned services. However, in this early stage of agent development, the agents and agent systems used are not yet very advanced, in other words they do not feature strong notions of agency. For the short-term, mediation services and query brokering are most relevant. In this early stage of agent development the use of agent technology is primarily aimed at providing logical and semantic interoperability between heterogeneous and disparate data sources. The primary effect this has on surveillance is that it is easier for law enforcement agencies to 'connect the dots' and make sense of massive amounts of data. Especially (distributed) data-mining exercises benefit from the use of agent technology. Both subject-based inquiries and pattern-based inquiries become more effective when agent technology is used. This will in turn empower surveillance operators and law enforcement officers.

It is my belief that in the medium to long-term future agent technology will be used to take over many of the surveillance tasks currently executed by human surveillance operators and law enforcement officers. Furthermore, since surveillance will become ubiquitous in the ambient-intelligence paradigm, software agents will be used to integrate previously discrete surveillance systems to an increasing extent. In this environment agents can be used for

a range of purposes, most notably automated monitoring tasks and decision-support tasks.

When in the long-term future strong artificial intelligence becomes a reality, software agents will become even more potent surveillance tools, taking over difficult surveillance tasks that up until now require human-level intelligence. In this phase it is possible, for instance, that we will see undercover software agents engaging in meaningful conversation with potential suspects.

From this section we may conclude that software agents will enhance the scope, effectiveness and efficiency with which surveillance can be conducted. Furthermore, by using agent technology the scope of surveillance can be broadened. In summary we can say that the use of agent technology for surveillance purposes will make surveillance more effective, efficient, and complete. It is my opinion that this development may have serious ramifications for privacy and (individual) liberty, which brings us to the second research question.

10.3 The impact of agent-enabled surveillance

On the basis of the conclusions of section 10.2 we can start to answer the second research question: *How will the use of agent technology impact privacy and liberty?*

In chapter 7 we have established that the use of agent technology will have both quantitative effects and qualitative effects on surveillance. The quantitative effects that can be associated with the use of agent-enabled surveillance are: (1) more efficient data gathering, (2) more effective data exchange and data mining, (3) system integration, (4) empowerment of surveillance operators, and (5) the replacement of surveillance operators. The qualitative effects that can be associated with agent-enabled surveillance are concerned with (1) competence and authority, (2) emergent behaviour, (3) transparency and insight, (4) adaptation, and (5) the strength of the agent metaphor.

The ubiquitous surveillance infrastructure so characteristic of the ambient-intelligence paradigm will become a valuable resource for law enforcement and intelligence agencies over the coming years. However, the enormous volumes of data will further intensify the problem of the information overload. It is likely that agent technology will be employed to make sense of the enormous amounts of data generated in the ambient-intelligence paradigm. The most notable result of this development is that the accessibility of information increases. As a result the quantitative and qualitative effects of agent technology on surveillance will be amplified. As we have seen in subsection 9.1.3 an increase in the availability (i.e., the ubiquitous surveillance infrastructure of the ambient-intelligence paradigm) and the accessibility of information (as a result of agent technology) will have a negative influence on privacy.

However, in my opinion the impact of agent technology on our (individual) liberty will be even more significant.

There is a strong drive in our culture towards higher levels of control and technologies that can help increase control are pursued vigorously. Security-related technology is a growth industry, in which artificial-intelligence research features prominently (Krikke 2006, p. 102). This drive towards more control is first and foremost the result of our modern scientific and technological worldview. Besides this underlying philosophical reason we also see that in general there is a great desire for speed, convenience, efficiency, and risk-management in our market-driven economies. This desire has led to the creation of many liberal surveillance infrastructures that facilitate modern life in the information society. But apart from the market-driven desire towards more control we also see a desire on the part of the state to enhance control for the purpose of ensuring national security. For a large part this desire can be contributed to the spectre of international terrorism. In an attempt to prevent a devastating terrorist attack, governments turn to electronic surveillance technology. As such, we can discern a rise in disciplinary surveillance, both in the public space and in cyberspace. While international terrorism is one of the main reasons for an increase in disciplinary surveillance, it is by no means the only reason. There is a general tendency on the part of the government towards social control. Moreover, the issue of 'function creep' can result in surveillance infrastructures and investigative powers being used for purposes for which they were not originally intended. As such we see the use of disciplinary surveillance for the purpose of social control in many places, most notably the public space.

In chapter 6 we have discussed two concepts of liberty, *viz.* negative liberty and positive liberty. While negative liberty is concerned with the absence of constraints, the positive concept of liberty is concerned with the ways in which desires are formed, whether as a result of rational reflection on all the options available, or as a result of pressure, manipulation or ignorance. It is my idea that without additional safeguards, positive liberty is at risk in the information society. The reason for this is that as more information about individuals becomes available due to ubiquitous surveillance, the ability to monitor and profile them increases. Thus, the extensive possibilities for data surveillance in the ambient-intelligence paradigm enhance the possibilities for social control. Moreover, since surveillance is becoming increasingly ubiquitous and software agents are excellent tools for (unobtrusive) monitoring, it is likely that panoptic effects will become stronger over time. It could thus be argued that we are moving towards a 'Superpanopticon' and that (in part) this Superpanopticon is made possible by agent technology. Keeping in mind the idea that knowledge is power, we can arrive at no other conclusion than that the arrival of the ambient-intelligence paradigm and the use of agent technology within this paradigm for disciplinary purposes is a potential threat to (positive) liberty.

So, the general conclusion we may draw is that agent technology will have significant impact on both privacy and liberty (in particular liberty in the positive sense). This situation can only be countered by creating barriers for the use of surveillance in the law. However, the enactment of anti-terrorism bills in both the Netherlands and the United States have broadened the scope of surveillance and relaxed the rules for its application, thereby contributing further to the effects of (agent-enabled) surveillance on privacy and liberty. Which brings us to the third research question.

10.4 THE IMPACT OF AGENT-ENABLED SURVEILLANCE ON THE LEGAL FRAMEWORK

The third research question for this thesis was formulated as follows: *How will the use of agent technology impact the legal framework for the protection of privacy and liberty?*

Agent technology can have quantitative and qualitative effects on surveillance, which in turn will impact the legal framework. The most significant consequences of these effects are: (1) that they will force us to rethink the legal framework, in particular the right to privacy, and (2) that they will prompt a need for new rules to deal with the qualitative effects of surveillance.

In the previous section we have established that the most significant effect of agent-enabled surveillance is its negative effect on positive liberty. The current way of mitigating the negative effects of electronic surveillance on liberty is by invoking the right to privacy. The role the right to privacy plays in shielding us from the observing gaze has been an important factor in safeguarding (individual) liberty. The importance of privacy in protecting liberty is clearly shown in the workings of the Panopticon: without privacy personal autonomy is nigh impossible. To this day the right to privacy is seen as the ideal candidate for shielding information about ourselves. With the arrival of electronic surveillance this line of thinking has been extended to include personal data, thereby including cyberspace as a dimension of the right to privacy.

However, over the course of this thesis we have also established that the right to privacy and personal data protection are unresponsive to the new reality of electronic surveillance. The reason for this is that the right to privacy has its origins in the physical world, with its focus on secrecy, concealment, and a clear distinction between the public and the private. When we examine the idea of personal data protection we see that the main problem is that it is focussed on individuals and the notion of an identifiable person, which is not necessarily an effective approach when it comes to agent-enabled surveillance in the ambient-intelligence paradigm. Over the course of its existence the right to privacy has changed many times in response to technological

changes. However, I believe that the right to privacy should not be reinvented once again in response to the arrival of agent-enabled surveillance and the ambient-intelligence paradigm. In my opinion, the idea that through the right to privacy we can retain our (individual) liberty in the slowly emerging 'ambient-intelligence Superpanopticon' is ultimately false.

Apart from their contribution to more effective and efficient electronic surveillance, software agents have several unique characteristics that will give rise to specific legislative issues. These issues are concerned with (1) the legal status of software agents, (2), jurisdiction, (3) transparency and accountability, and (4) limitation of their use. Since the legal framework for the protection of privacy and liberty was conceived before surveillance technologies came into being that could display characteristics such as autonomy, emergent behaviour, adaptability and mobility, it is not well suited for dealing with the qualitative effects of agent technology. If these issues are not addressed in the legal framework legal certainty and consequently privacy and liberty are at risk.

The quantitative and qualitative effects of agent-enabled surveillance manifest themselves in both the legal framework of the Netherlands and the United States. The way these effects influence the legal framework however differs somewhat between the Netherlands and the United States.

When we examine the legal framework of the Netherlands (civil law) we see that it suffers from the problems with the right to privacy as described in this thesis. As such the quantitative effects of agent technology are not adequately addressed in the legal framework of the Netherlands. In the legal framework of the Netherlands the second line of privacy theory, which focuses on the control of personal data, predominates. While the principles of data protection are important in safeguarding privacy and liberty, the focus on *personal* data is too strong in the Netherlands. Moreover, recent changes in the law of criminal procedure, which allow for the more liberal gathering of private sector data will provide an additional threat in the light of agent-enabled surveillance. Furthermore, the qualitative effects of agent technology are not addressed in the legal framework of the Netherlands.

When we examine the legal framework of the United States (common law) we see that it too suffers from problems with the right to privacy. As such the quantitative effects of agent technology are not adequately addressed in the legal framework of the United States. In the United States the first line of privacy theory, which focuses on notions of the private sphere, predominates. This line of privacy theory makes a clear distinction between the public sphere and the private sphere, and as such the reasonable expectation of privacy criterion is of particular importance in the legal framework of the United States. However, we have established that this criterion can provide little protection in the ambient-intelligence paradigm. Moreover, the fact that data may be gathered more or less freely in the public sphere and the fact that less procedural requirements exist in the United States when it comes

to sharing data, means that privacy and (individual) liberty are at risk. Furthermore, the qualitative effects of agent technology are not addressed in the legal framework of the United States.

In summary, we may say that both the legal framework of the Netherlands and the United States need revision in the future if they are to deal effectively with the issue of agent-enabled surveillance, which brings us to the fourth research question.

10.5 The regulation of agent-enabled surveillance

In this thesis I have argued that the use of agent technology may influence surveillance in both a quantitative manner and a qualitative manner and that these effects may influence privacy and liberty in an adverse way. I have also discussed why I feel that the current legal framework is unable to deal with the quantitative and qualitative effects of agent technology. This leaves me to answer the fourth research question: *In order to safeguard privacy and liberty, how must the use of software agents be regulated?*

Over the course of this thesis we established that the surveillance net is being cast wider through changes in substantive law and the law of criminal procedure, and that the meshes are thinned through increasingly effective (agent-enabled) electronic surveillance. Both the quantitative effects and qualitative effects of agent-enabled surveillance on privacy and liberty are difficult to predict and to measure. Furthermore, the 'surveillance sorites paradox' and the problem of the slippery slope described in chapter 8 make normative choices about the regulation of agent-enabled surveillance difficult. This is especially true for quantitative effects of agent technology that do not form a radical break with past surveillance practices. In a sense, we must choose a point on the slippery slope where we feel that there is no longer an adequate level of privacy and liberty. Such a choice is difficult -if not impossible- to make due to the fact that the predicate 'an adequate level of privacy and liberty' is indeterminate, and any choices regarding it will be highly subjective. Moreover, privacy and liberty are not isolated factors: they must be viewed in the context of other values and interests in society.[2] As such placing an absolute value on what is an adequate level of privacy and liberty is not possible in my opinion.

What we can do is ensure that the necessary mechanisms are in place that help protect privacy and liberty. We have seen that in order to protect privacy and liberty the legal framework must meet certain general requirements. A first requirement is clear substantive criminal law. The more vague substantive

2 The fact that privacy and liberty must be viewed in the context of other values and interests in society does not imply they must be balanced with these values in a zero-sum game.

criminal law is formulated, the more room there is for discretionary authority in the application of investigative powers. A second requirement is that the use of agent-enabled surveillance must adhere to the principle of legality. This means that the legal status of agent-enabled surveillance and its qualification as an investigative power must be sufficiently clear and preferably its use must be based on a specific statutory provision. Since agent technology is such a potent surveillance tool, a third requirement is that the use of agent-enabled surveillance must meet the standards of proportionality and subsidiarity. The fourth requirement is also related to the power of agent-enabled surveillance and is concerned with the limitations on the use of agent technology. A fifth requirement is the transparency and accountability of agent-enabled surveillance. Finally, the right to participation is a sixth requirement for the use of agent technology. Apart from these general requirements we have established that we must find legislative solutions to the quantitative and qualitative effects of agent technology.

When it comes to the quantitative effects of software agents we have established that we must address the questions they raise in the broader context of electronic surveillance, privacy, and liberty. In the light of the quantitative effects of agent-enabled surveillance I feel it is of particular importance to leave the right to privacy as a primary means of defending liberty. In my opinion we must come to the realisation that the protection of privacy is not the primary issue, rather it is how the use of electronic surveillance and data derived thereof (regardless of the fact that these data can be characterised as personal data) influences the balance of power between the observers and the observed.

Within the general discussion about surveillance, privacy and liberty, the processing of surveillance data takes up an important place. The main question (a threefold question) we must ask ourselves when it comes to the processing of surveillance data is: who may use surveillance data, under what circumstances and for which purposes? While this question underlies current data protection legislation to a certain extent, it is my idea that we must move beyond the idea that data protection is predominantly an issue of privacy. This means that we must lessen the focus on *personal* data in current data protection legislation. The question is not how the use of personal data affects our (informational) privacy, but rather how the use of data in general can influence our individual liberty and that of society as a whole.

These ideas are not easily translatable to the legal framework. Since discarding privacy as the primary bulwark against (electronic) surveillance forms such a departure from the current norm, careful deliberation and further discussion on this topic is necessary. As mentioned in chapter 8 choices regarding the content and structure of the legal framework that are aimed at dealing with the quantitative effects of agent technology are primarily of a normative nature. The normative choice that must be made is the following:

how effective do we allow agent-enabled surveillance to become?[3] Since an answer to this question will be formulated in the political arena, I feel it is of particular importance that all the relevant actors have an understanding of how agent-technology works, and what its likely effects on privacy and liberty are. Furthermore, the actors involved should grasp the fact that the right to privacy is no longer the most effective method of addressing the issues associated with electronic surveillance in general and agent-enabled surveillance in particular. In my opinion the most important step we must therefore take in addressing the quantitative effects of agent-enabled surveillance is raising awareness about this issue in society, thereby providing a solid basis for further discussion.

We have established that organisational and technological barriers to electronic surveillance will become progressively less of an obstacle in the future. Thus, if we want to limit the effectiveness of electronic surveillance we have to do so through changes in the law. As we have seen in chapter 9 the law can restrict the use of agent-enabled surveillance in several ways. Based on the normative choices regarding the use of agent technology, we can implement measures for limitations on the use of agent-enabled surveillance. Such a first step includes limitations on the scope of agent-enabled surveillance, the duration of agent-enabled surveillance, and the authority of surveillance operators and law enforcement officers to use agent-enabled surveillance.

The rules regarding the use of agent-enabled surveillance are most effective once they are incorporated into the technology itself. Through technologies, such as rule-based processing, selective revelation, and strong credential and audit mechanisms, we ensure that the rules for the use of agent-enabled surveillance are actually effectuated. The notion of normative agents is particularly relevant in this regard.

A second important step in safeguarding (individual) liberty in the light of agent technology is ensuring that the technology is not only available to those in power. By providing agent technology to citizens we open up the possibility of synoptic or reciprocal transparency, which could aid in restoring the balance of power between the observers and the observed. By opening up the possibility of effective synoptic surveillance we can give an answer to the question: "Quis custodiet ipsos custodes?"[4] Furthermore, by creating a higher degree of transparency we can avoid the negative consequences of the 'unseen Panopticon'.

When it comes to a discussion about the qualitative effects of agent technology we see that a clear legal status of agent-enabled surveillance forms a crucial starting point. On the basis of the legal status of software agents we can decide in which cases the use of agent-enabled surveillance is warranted.

---

3 I shall give my personal view on this normative issue when I draw my final conclusions in section 10.6.

4 This latin phrase from a play by Iuvenalis (Juvenal) translates as follows: *"Who shall guard the guardians?"*.

Furthermore, a statutory basis for the use of agent-enabled surveillance would provide room for the further regulation of the qualitative effects of agent technology, such as jurisdiction, transparency and accountability, and use limitation. As opposed to the quantitative effects of agent technology, these qualitative effects can be addressed by means of changes to the existing legal framework.[5]

As with the quantitative effects of agent-technology use limitation features prominently. As such rules that govern the scope and duration of agent-enabled surveillance as well as the authority to use it must be clearly defined. However, when we talk about the qualitative effects of agent technology we can see that we are facing an additional problem: *how do we limit the use of agent-enabled surveillance applications whose operation is difficult to predict?* Or, in other words: how do we deal with the specific characteristics of agent technology (i.e., autonomy, emergent behaviour, and adaptability,) that create uncertainty with regards to their operation. When it comes to the specific characteristics such as autonomy, emergent behaviour, and adaptability we see that there are basically two choices: either we (1) limit the autonomy of agents, their ability to adapt, and their ability to display emergent behaviour in the legal framework (thereby negating the effectiveness of these advanced agents), or (2) we accept a certain level of uncertainty (thereby increasing the effectiveness of agent-enabled surveillance but decreasing legal certainty).

10.6 FINAL CONCLUSIONS

The main goal of this thesis has been to identify the threats that software agents may pose to privacy and liberty. Moreover, I have explored ways of ensuring the best possible protection against these threats. The problem definition of this thesis was formulated as follows: *Is it possible to maintain privacy and liberty in a society where software agents are able to overcome the information overload?* In this section I shall try and answer the problem definition and draw my final conclusions.

The central theme of this thesis has been that knowledge is power. As such, it has concerned itself with the impact of electronic surveillance on the individual and society. As part of the broader evolution of science and technology we can establish that the rise of electronic surveillance is primarily concerned

5 A good example of a legal issue related to the qualitative effects of agent technology that would benefit from a clear legal status of agent-enabled surveillance is the issue of jurisdiction. We have established that the nationality of a software agent must be identifiable if we want to address issues of jurisdiction. By giving agent-enabled surveillance a clear legal status (for instance as an investigative power) we can stipulate in the rules that govern its use that the nationality of an agent (or that of its user) must identifiable.

with risk-management, rationalisation, and control. We established that there is a strong drive in our culture towards attaining these goals, and that tools like software agents can aid in realising them. In this sense the ability of agent technology to facilitate control and society's wish for greater security and risk-management are mutually strengthening occurrences.

In the law of criminal procedure of both the Netherlands and the United States we see that the rules for the application of investigative powers have been relaxed and that there is a greater emphasis on pro-active investigation, which means that investigative methods and powers can be applied in an earlier stage. Since the scope of substantive criminal law is pushed forward (i.e., before an actual criminal act has actually taken place) invasive investigative methods can be applied in an early stage.

This brings us back to the issue of agent-enabled surveillance and the problem definition of this thesis. The arrival of agent-enabled surveillance will magnify the current trend towards risk justice, since it will deliver the tools necessary to effectuate it. While the use of agent-enabled surveillance may benefit national security and help reduce crime, I feel that we should be very cautious not to use agent-enabled surveillance over-extensively. In my opinion the three interrelated developments mentioned above are a cause for concern. As we have established earlier in this thesis, the changes in substantive criminal law and the law of criminal procedure have already expanded the surveillance net, while the use of agent-enabled surveillance will thin the meshes of this net considerably in the near future. Heidegger (1953) argued that the essence of technology is the methodical planning of the future, and that as result a new type of cultural system would emerge that would restructure the entire world as an object of control. Judging from the developments in the area of criminal law and surveillance technology, I feel Heidegger's observation is accurate. The notion of risk justice strengthened by the use of agent-enabled surveillance opens up the possibility of extensive social control and orchestration. In particular, the panoptic effects that may arise as a result of these developments are detrimental to (individual) liberty.

Does this mean it is impossible to maintain adequate levels of privacy and liberty when software agents are able to overcome the information load? Not necessarily in my opinion. Judging from the conclusions drawn over the course of this thesis we can establish that with appropriate safeguards in the legal framework (effectuated in technology and procedures) it is possible to maintain privacy and liberty in a society where software agents are able to overcome the information overload. However, ensuring that the appropriate safeguards are put in place will require a critical attitude from lawmakers and policy-makers, something that in my opinion is currently lacking in the discussion about the application of electronic surveillance. When it comes to making choices about the application of surveillance, the classic dichotomy is that of

privacy versus security.[6] In this discussion privacy is almost always sacrificed in favour of enhanced security. However, the effects agent-enabled surveillance may have on (positive) liberty should not be underestimated. I hope that by giving rights and values other than the right to privacy a more prominent place in the discussion about national security, we can have a more balanced debate. If the law is to fulfil its vital role in society we must accept the fact that its not only there to manage risks and enhance (national) security, but that it is also there to ensure liberty, equal treatment, and social cohesion.

With the very real threat of international terrorism it is important that the intelligence community and law enforcement agencies have the appropriate tools for preventing attacks. Therefore, it is important that the possibilities of agent-enabled surveillance are pursued further. But at the same time we must also pursue the goals of privacy and liberty. This means adjusting the legal framework to meet the demands of new technological realities. As discussed throughout this thesis, it is my opinion that the role of privacy in the protection of liberty is too great in the current legal framework. However, this does not mean we must abandon the right to privacy in favour of an entirely new system of protection. In my opinion there is no single alternative to the current legal framework for the protection of privacy and liberty. Rather it is my view that we must shift the balance from the right to privacy towards other means of protection somewhat. The mechanisms mentioned in chapter 9 would strengthen the current legal framework and provide additional protection alongside the right to privacy.

At this point in time, the potential impact of agent-enabled surveillance on individuals and society is not yet clearly understood. If we are to maintain adequate levels of privacy and liberty in the future, we must gain a greater understanding of the effects of agent-enabled surveillance. Which brings me to my suggestions for future research.

10.7 Suggestions for future research

In this thesis I have discussed the issue of agent-enabled surveillance, privacy, and liberty on a more or less abstract level. While I have formulated answers to several important questions, this thesis raises far more questions in various scientific fields than it can answer. Moreover, I have made suggestions about possible solutions to the problem definition of this thesis (both of a legislative and a technological nature) that need to be explored further. Therefore, I shall give some suggestions for future research in the area of agent-enabled surveillance, privacy and liberty below.

---

6 Personally I agree with the view of Taipale set forth in section 8.5.1, *viz.* that privacy, liberty, and security are values that should all be maximised instead of traded for one another in a zero sum game.

More research needs to be done concerning the future of electronic surveillance and its effect on privacy, but more importantly on (individual) liberty. In this thesis I have explored the issue of agent-enabled surveillance, which is actually only a small part of the broader issue of electronic surveillance, privacy and liberty. Much like I have tried to do in this thesis, further research should bring together insights from various fields of scientific inquiry. Our suggestions for future research therefore covers four areas, *viz.* psychology, sociology, computer science, and the law.

First, in the area of psychology and sociology I feel more research should be done on the effects of electronic surveillance on (individual) liberty. It is of particular interest to determine if, how, and when panoptic effects of electronic surveillance manifest themselves. Since the ambient-intelligence vision is not yet realised, it is difficult to get any empirical data on panoptic effects of electronic surveillance in society as a whole. However, by studying the effects of electronic surveillance in closed environments such as the workplace and the prison we can get an image of the panoptic effects of electronic surveillance.

Second, in the area of computer science more research must be done on finding ways of incorporating the rules of the legal framework into surveillance technology. In my opinion the idea of normative agents holds much promise and must be examined further. Apart from research into normative agents, methods for the identification, authentication, and authorisation of software agents need to be explored. Moreover, technological solutions to transparency and accountability, of which logging mechanisms feature prominently, need to be researched. Furthermore, technologies should be explored that could give greater meaning to the right to participation and the ability for synoptic surveillance.

Third, in the area of the law, additional study into the quantitative and qualitative effects of agent-enabled surveillance on the legal framework is necessary. In particular, additional research should be done on legislative alternatives for the right to privacy in the protection of liberty. Finally, possible changes to the legal framework that are necessary to deal with the qualitative effects of agent technology should be examined further.

Summary

This thesis is concerned with the use of software agent technology for surveillance purposes and its possible effects on privacy and liberty. The goal of the thesis is to determine whether the current legal framework for the protection of privacy and liberty in the Netherlands and the United States is adequately suited to address the negative effects of agent-enabled surveillance.

In the fight against terrorism and organised crime, technologies such as CCTV, data mining, radio frequency identification (RFID), autonomous systems, and biometrics are used to increasing extent. The driving force behind this development is the importance of information. Knowledge on a particular subject enhances our understanding and enables us to exercise more control. Bacon (1597) has summarised this idea in the now famous adage *knowledge is power*. However, the September 11 terrorist attacks showed that only gathering massive amounts of data is not sufficient to prevent an attack. While there were sufficient data available that suggested a large-scale attack was imminent, the authorities were unable to act upon these data. One of the main reasons for this inability was that the sheer volume of the available data made a transformation into information and knowledge difficult. This problem is known as 'information overload'.

Artificial intelligence plays an important role in reducing the information overload. This thesis focuses on the use of software agents for surveillance purposes. Software agents are intelligent computer programs that are able to perform a task without direct human supervision (see chapter 2). When it comes to surveillance, software agents can be used for: (1) the collection of data, (2) data mining, (3) automated surveillance (most notably of the public sphere), and (4) decision support (see chapter 4).

While the use of agent technology holds great promise for combating terrorism and organised crime, it also raises questions about the 'information power' the government can derive from its use. Government surveillance can alter the balance of power between the government and its subjects since the knowledge garnered by means of surveillance can be misused or abused to exercise control. This can be direct control, but also an indirect mode of control that is the result of 'panoptic feelings'. These feelings arise when an individual

is under the impression that his behaviour is continuously monitored.[1] As a result of this monitoring, the individual will oftentimes alter his behaviour in order to comply with the social norm.[2] It makes the mere presence (or perceived presence) of a surveillance infrastructure a means to exercise some form of social control (see chapter 3).

In order to address the possible negative effects of electronic surveillance the right to privacy is oftentimes invoked (see chapter 5). However, privacy is not a static object that can be captured and defined, it is always context related. This has led to different conceptions of privacy (such as privacy as limit to power and privacy as emotional release) and different dimensions of the right to privacy (such as the home and the correspondence).

Apart from examining the right to privacy it is also necessary to shed more light on the concept of liberty. It is helpful to make a distinction between 'negative liberty' and 'positive liberty'. Negative liberty is the absence of external influences and constraints, while positive liberty is the ability on the part of the individual to determine for himself his own course of action (see chapter 6).

Currently there are several socio-technical inhibitors and practical limitations to the development of a fully functioning, all encompassing, surveillance network (Innes 2003). The three most important inhibitors are a lack of inter-organisational cooperation, legal barriers, and technical issues. But agent technology is rapidly removing this barrier, which brings us to the problem definition of this thesis:

Is it possible to maintain privacy and liberty in a society where software agents are able to overcome the information overload?

To answer this problem definition we must first establish what the effects of agent technology on surveillance are. Next, we must examine to whether the current legal framework for the protection of privacy and liberty is able to deal with these effects.

The possible effects of agent technology on surveillance, privacy, and liberty can be divided into two categories: the *quantitative* effects of agent technology and the *qualitative* effects of agent technology (see chapter 7). Quantitative effects of agent technology are those effects that do not form a break with past surveillance practices and their effects on privacy and liberty. The quantitative effects of agent-enabled surveillance add to an ongoing situation of intensifying surveillance. Qualitative effects of agent technology are those effects that that raise specific questions with regard to privacy and liberty. Owing to some of their unique characteristics, software agents might influence the surveillance

1 For the sake of brevity I will use in this thesis only the male gender of nouns and pronouns in all cases where the person referred to could be either male of female.

2 Panoptic feelings can also arise in groups.

practice in such a way that their application will yield effects currently unimagined. Among the unique characteristics likely to influence surveillance in the future are: autonomy, emergent behaviour, adaptive capabilities, and mobility.

The five quantitative effects that are discussed in chapter 7 of this thesis are: (1) more efficient data monitoring and data gathering, (2) more effective data exchange and data mining, (3) system integration, (4) empowering surveillance operators, and (5) replacing surveillance operators.

The five qualitative effects that are discussed in chapter 7 of this thesis are: (1) competence and authority, (2) emergent behaviour, (3) adaptation, (4) transparency and insight, and (5) strength of the agent metaphor.

The quantitative and qualitative effects will both influence the legal framework for the protection of privacy and liberty, albeit in different ways. For this reason we must differentiate between the two types of effects when it comes to judging whether the legal framework is still adequate.

Quantitative effects

The quantitative effects of agent-enabled surveillance primarily lead to a change in the scale of surveillance. This will raise questions as to how the balance should be struck between surveillance and security on the one hand and privacy and liberty on the other hand.

In my opinion, the ongoing development of the information society, where personal data is processed to an increasing extent, in combination with the development of agent technology, will place additional pressure on the legal framework. In the future, the distinction between the public sphere and the private sphere will become increasingly hard to make. In my opinion the importance of the right to privacy should therefore be reduced significantly in the legal discourse.

The right to privacy fulfils an important role in limiting the power that can be exercised over individuals and groups. In this conception of the right to privacy, privacy itself is not a goal, but rather a means to a different end, *viz.* liberty. It is my opinion that the current pre-occupation with the right to privacy (in particular in the political discourse) oftentimes masks the actual problem, namely the erosion of liberty. This even more harmful since in the information society the right to privacy has several weaknesses. These weaknesses are: (1) an inherent vagueness and dependence on context, (2) a necessary distinction between the public and the private sphere, (3) subjective interpretations and expectations surrounding the right to privacy, (4) the characterisation of privacy as an individual right, and (5) 'bad publicity' surrounding the right to privacy.

Already these weaknesses of the right to privacy cause problems when it comes to its application in the information society, problems that will become more acute as a result of agent technology. Therefore, it is my opinion that the right to privacy and its role in defending liberty needs to be re-evaluated.

In particular more attention needs to be devoted to other fundamental rights and freedoms such as the freedom of speech.

Qualitative effects

The qualitative effects of agent technology raise questions with regard to: (1) the legal status and qualification of investigative powers, (2) jurisdiction, (3) transparency and accountability, and (4) use limitation.[3] These questions are not addressed in the current legal framework since it was put into place before the advent of agent technology.

The first and in my opinion most important question regarding the qualitative effects of agent-enabled surveillance is their legal status and qualification as an investigative power. Software agents are capable of intelligent and autonomous action, but the question is whether they are allowed to do so.

The second question is related to the jurisdiction of software agents. Given the international character of the internet, the autonomy of software agents, and their mobility, it is likely that software agents will carry out cross-border surveillance. In these cases it is important to set clear rules for the jurisdiction of software agents.

The third question raised by the qualitative effects of agent technology is the transparency and accountability of their actions. Since agents are autonomous their actions are not always transparent. The adaptability of agents and the possible emergent behaviour add to this situation. Moreover, in general software agents and agent-systems are complex and therefore their actions can be difficult to predict or monitor.

The fourth question raised by the qualitative effects of agent technology is that of use limitation. This question is closely related to the first and third question and is the result of characteristics such as autonomy, adaptability, and emergent behaviour. In theory, these characteristics enable software agents to query any number of databases and other information sources. It is thus necessary to set rules that limit their freedom of movement. Currently these rules are lacking.

Judging from these previous considerations it is likely that the legal framework for the protection of privacy and liberty will come under increasing pressure. Therefore, it is important to determine how the legal framework should develop in the future. Possible changes to the legal framework must also be effectuated in technology and accompanying procedures (see chapter 9).

The regulation of agent technology must meet some basic criteria (see chapter 8). For the most part these criteria are already part of the legal discourse. They are (1) the principle of legality, (2) a clear substantive criminal law, (3) proportionality and subsidiarity, (4) equal treatment under the law, (5) use limitation, (6) transparency and accountability, and (7) the right to participation.

---

3 The strength of the agent metaphor does not raise any legal questions in itself.

Apart from the basic criteria, specific adaptations must be made to the legal framework to deal with the specific effects of agent technology.

It is difficult to deal with the *quantitative* effects of agent technology through legislation. The reason for this is that it is difficult, if not impossible, to determine what an adequate level of privacy is. As such agent-enabled surveillance finds itself on a 'slippery slope'. There are however some mechanisms to counter the quantitative effects of agent-enabled surveillance.

A first mechanism is raising awareness about agent-enabled surveillance and its possible effects on privacy and liberty. A second mechanism is devoting more attention to the fundamental rights that up until now have depended primarily on the right to privacy for their protection. A third mechanism is implementing laws and regulation in technology and procedures (privacy enhancing technologies and privacy by design). In this area the notion of normative agents is particularly relevant. A fourth mechanism is ensuring that some extent citizens can gain knowledge on the surveillance practices of their government.

With regard to the *qualitative* effects of agent technology it is of particular importance to clarify the legal status of agent-enabled surveillance. A clear legal status forms the basis for implementing specific rules for dealing with the qualitative effects of agent-enabled surveillance.

In my opinion there are four options when it comes to giving software agents a legal status, *viz.* (1) an agent is seen merely as an investigative tool, (2) the authority of the agent is based on that of its user, (3) we view the use of agents as a special investigative power, or (4) agents receive a separate status in the law of criminal procedure. The choice for any of these options is for a large part dependent on the actual impact of the agent technology used. We can state that when agents have higher levels of intelligence and autonomy, their impact on privacy and liberty is potentially higher. The use of these agents should be subjected to stricter rules, something that should be reflected in their legal status.

We may conclude that software agents will make the exercise of surveillance more effective and efficient, a development that may threaten privacy, but more importantly liberty. As a result of a more complete agent-enabled surveillance infrastructure and accompanying panoptic feelings, it is mainly positive liberty that is threatened, whereas up until now, it was mainly negative liberty that was at stake. Furthermore, we may conclude that the current legal framework for the protection of privacy and liberty, which is primarily focused on the right to privacy, will no longer suffice in our agent-enabled future. Still, it is my opinion that with the proposed changes to the legal framework the quantitative and qualitative effects of agent technology can be adequately addressed.

Samenvatting

SOFTWARE AGENTEN, SURVEILLANCE EN PRIVACY: EEN JURIDISCH KADER VOOR DE TOEPASSING VAN SOFTWARE AGENTEN IN DE OPSPORING

Dit proefschrift houdt zich bezig met het gebruik van software agenten voor surveillance doeleinden en de gevolgen die dit kan hebben voor de privacy en vrijheid van burgers. In het proefschrift wordt gekeken in hoeverre het huidige juridisch kader voor de bescherming van de privacy en vrijheid in Nederland en de Verenigde Staten is toegerust om de mogelijke negatieve effecten van het gebruik van software agenten voor surveillance doeleinden het hoofd te bieden. Voorts worden suggesties gedaan om het juridisch kader te verbeteren en de risico's bij het gebruik van software agenten te minimaliseren.

Bij de bestrijding van terrorisme, (georganiseerde) criminaliteit en de handhaving van de openbare orde wordt steeds vaker gebruik gemaakt van technologische hulpmiddelen. Technologieën als videocamera's, data mining, radio frequency identification (RFID), autonome systemen en biometrische identificatie moeten het hoofd bieden aan nieuwe bedreigingen en de veiligheid van onze maatschappij helpen vergroten. De drijvende kracht achter de introductie van veel van deze technologieën is het toenemende belang van informatie. Kennis over een bepaald proces, een object of een situatie stelt ons in staat om het voorwerp van onze kennis te begrijpen en te controleren. Bacon (1597) heeft dit kernachtig samengevat in wat wij nu kennen als het adagium *kennis is macht*. Het verzamelen van informatie is uiteraard altijd van belang geweest bij het handhaven van de (nationale) veiligheid. De onverwachte aanvallen op het World Trade Center en het Pentagon in september 2001 toonden echter aan dat het eenvoudigweg verzamelen van grote hoeveelheden data niet voldoende was. Kennelijk ontbrak er een transformatie, namelijk het omzetten van data in relevante informatie. Een belangrijke oorzaak van dit probleem was dat de politie- en veiligheidsdiensten moeilijk hun weg konden vinden in de grote hoeveelheden beschikbare data. Dit probleem staat bekend als *information overload*.

Kunstmatige intelligentie speelt een voorname rol bij het bestrijden van *information overload*. In het kader van dit proefschrift is met name de ontwikkeling van software agenten relevant. Een software agent is een intelligent programma dat zonder directe tussenkomst van de mens kan handelen. De voornaamste toepassingen van software agenten in het kader elektronische

surveillance zijn: (1) het verzamelen van data, (2) het ontdekken van nuttige informatie in data (data mining), (3) het houden van geautomatiseerd toezicht (op de publieke ruimte) en (4) het ondersteunen van beslissingen (zie hoofdstuk 4).

Hoewel de toepassing van software agenten voor het bestrijden van georganiseerde misdaad en internationaal terrorisme een veelbelovende ontwikkeling is die de veiligheid van onze maatschappij kan helpen vergroten, roept het gebruik van deze technologie ook vragen op met betrekking tot de 'informatiemacht' die de overheid kan ontlenen aan het gebruik van software agenten. Toezicht van de overheid op haar burgers (surveillance) kan de machtsbalans tussen de overheid en haar burgers verstoren. De kennis die ontleend kan worden aan surveillance kan gebruikt (of misbruikt) worden om controle over burgers uit te oefenen. Dit kan directe controle zijn, maar ook indirecte controle die het gevolg is van 'panoptische gevoelens'. Er is sprake van panoptische gevoelens wanneer personen onder druk van het idee dat hun gedrag geobserveerd kan worden dit gedrag aanpassen aan een bepaalde heersende norm. Hiermee wordt de enkele aanwezigheid van (elektronische) surveillance, of de mogelijke aanwezigheid ervan, een instrument om sociale controle uit te oefenen (zie hoofdstuk 3).

Om deze mogelijke negatieve aspecten van elektronische surveillance het hoofd te bieden wordt het recht op privacy ingeroepen. Een eenduidige definitie van het begrip privacy is moeilijk tot niet te geven. Dit komt hoofdzakelijk door het feit dat het begrip privacy slechts vorm krijgt door verwijzing naar een complex geheel van sociale, culturele, politieke, juridische en filosofische factoren waarvan het afhankelijk is (Gutwirth 1998). Het recht op privacy beschermt een nauwomlijnde, maar relatief onschendbare persoonlijke levenssfeer tegen bemoeienis van buitenstaanders (Blok 2002). In dit kader kan het recht op privacy onderverdeeld worden in een aantal concepties (wat tracht men met het recht op privacy te bewerkstelligen) en een aantal dimensies (waarop is het recht op privacy van toepassing). Tot de concepties van het recht op privacy behoren onder andere: het beschermen van de persoonlijke autonomie, het afsluiten voor invloeden van buitenaf en het mogelijk maken van sociale interactie. Tot de dimensies van privacy behoren onder andere: het lichaam, het huis, communicatie en het familieleven (zie hoofdstuk 5).

Met het oog op het onderwerp van dit proefschrift is het noodzakelijk om naast het begrip privacy ook het begrip vrijheid nader te definiëren. In dit kader werkt een onderscheid tussen 'negatieve' en 'positieve' vrijheid verhelderend. Negatieve vrijheid is de afwezigheid van invloeden van buitenaf, terwijl positieve vrijheid geassocieerd wordt met de mogelijkheden om jezelf volledig te ontplooien. Naar mijn mening zijn beide vormen van vrijheid in het geding bij het gebruik van software agenten voor surveillance doeleinden (zie hoofdstuk 6).

Momenteel bestaan er een aantal barrières die een effectieve surveillance infrastructuur in de weg staan en daarmee privacy en vrijheid beschermen

(Innes 2003). Het gaat om: (1) institutionele barrières, (2) technische barrières, en (3) juridische barrières.

De eerste twee barrières zorgen voor een *de facto* bescherming van de privacy en vrijheid. Echter, met de komst van kunstmatige intelligentie in het algemeen en software agenten in het bijzonder, worden deze barrières in een rap tempo geslecht, wat ons brengt bij de probleemstelling van dit proefschrift:

Is het mogelijk om privacy en vrijheid te handhaven wanneer software agenten in staat zijn om de information overload als barrière voor effectieve surveillance te slechten?

Om deze vraag te kunnen beantwoorden moeten we allereerst vaststellen wat de effecten van software agenten op de surveillance zijn. Vervolgens moeten wij kijken in hoeverre deze effecten ondervangen kunnen worden in het huidige juridisch kader voor de bescherming van de privacy en vrijheid.

We kunnen de mogelijke effecten van agenttechnologie op de surveillance verdelen in twee categorieën. Enerzijds zal het gebruik van agenttechnologie een *kwantitatieve* invloed hebben op surveillance, privacy en vrijheid. Anderzijds zal het gebruik van autonome systemen een *kwalitatieve* invloed hebben op surveillance, privacy en vrijheid (zie hoofdstuk 7). Deze effecten zullen op hun beurt het juridisch kader beïnvloeden.

Kwantitatieve effecten van door agenttechnologie ondersteunde surveillance zijn die effecten die qua uitwerking geen radicale breuk vormen met andere vormen van elektronische surveillance en hun gevolgen. In feite gaat het hier om effecten die zorgen voor een schaalvergroting: door het gebruik van software agenten wordt elektronische surveillance efficiënter en effectiever. *Kwalitatieve effecten* van door agenttechnologie ondersteunde surveillance zijn toe te schrijven aan de unieke technische eigenschappen van agenttechnologie zoals autonomie, emergent gedrag en zelflerend vermogen. Deze eigenschappen beïnvloeden de surveillance dusdanig dat zij specifieke vragen oproepen met betrekking tot privacy en vrijheid.

De vijf kwantitatieve effecten die in dit proefschrift worden besproken zijn: (1) een toename in het toezicht op en het verzamelen van data, (2) een toename in de toepassing en effectiviteit van data mining, (3) integratie van surveillance systemen, (4) het versterken van de capaciteiten van surveillance operators en (5) het vervangen van surveillance operators door software agenten.

De vijf kwalitatieve effecten die in dit proefschrift worden besproken zijn: (1) vragen rondom de bevoegdheden van agenten, (2) emergent gedrag van agenten (3) het zelflerend en aanpassend vermogen van agenten, (4) vragen rondom transparantie en inzicht en (5) de kracht van de agent metafoor.

De kwantitatieve en kwalitatieve effecten beïnvloeden het juridisch kader voor de bescherming van privacy en de vrijheid op verschillende wijzen. Om deze reden moet er bij de beoordeling van de houdbaarheid van het juridisch kader een onderscheid gemaakt worden tussen de invloed van de kwantitatieve

effecten op het juridisch kader en de invloed van kwalitatieve effecten op het juridisch kader (zie hoofdstuk 8).

Kwantitatieve effecten
De kwantitatieve effecten van agenttechnologie roepen niet zozeer nieuwe juridische vragen op, veeleer maken zij bestaande vraagstukken rondom surveillance, privacy en vrijheid meer acuut. De kwantitatieve effecten van software agenten zullen hoofdzakelijk invloed hebben op de vraag welke balans er moet zijn tussen effectieve surveillance- en opsporingsmethoden enerzijds en privacy en vrijheid anderzijds.

De voortschrijdende ontwikkeling van de informatiemaatschappij, waarin steeds meer informatie over personen kan worden vastgelegd, in combinatie met de ontwikkeling van agenttechnologie, zal naar mijn mening steeds meer druk leggen op het huidige juridisch kader voor de bescherming van privacy en vrijheid. In de toekomst zal het steeds moeilijker worden om de persoonlijke levenssfeer af te sluiten en zal het onderscheid tussen de publieke sfeer en de persoonlijke sfeer steeds verder vervagen. Het gevolg hiervan is dat het recht op privacy aan belang zal (moeten) inboeten.

Het recht op privacy vervult met name een belangrijke functie bij het limiteren van macht over onze persoon. In deze conceptie van het recht op privacy is privacy dus niet zozeer *doel* op zichzelf, alswel *middel* tot het bereiken van een ander doel, namelijk vrijheid. Ik ben van mening dat door de huidige preoccupatie met het recht op privacy (specifiek in het politiek discours) in veel gevallen het daadwerkelijke probleem, namelijk de limitering van onze vrijheid, uit het oog wordt verloren. Dit is schadelijk, daar het recht op privacy in de informatiemaatschappij een aantal zwaktes kent waardoor het niet altijd een effectief beschermingsmechanisme is (zie hoofdstuk 6). Deze zwaktes zijn: (1) een inherente vaagheid en afhankelijkheid van context, (2) de noodzakelijkheid van een onderscheid tussen de publieke sfeer en de private sfeer, (3) subjectieve interpretaties en verwachtingen rondom het recht op privacy, (4) de karakterisering van privacy als individueel recht, en (5) veel negatieve publiciteit en beeldvorming rondom privacy.

Deze zwakke punten zorgen nu reeds voor problemen bij de toepassing van het recht op privacy, een ontwikkeling die versterkt zal worden door de kwantitatieve effecten van agenttechnologie. Daarom zal naar mijn mening uiteindelijk een grondige herijking van het juridisch kader nodig zijn. Zo zal er onder andere meer aandacht moeten komen voor andere grondrechten zoals het recht op vrije meningsuiting en het recht op vergadering.

Kwalitatieve effecten
De kwalitatieve effecten van agenttechnologie op de surveillance roepen vragen op met betrekking tot: (1) de juridische status van software agenten en hun kwalificatie als opsporingsbevoegdheid, (2) de jurisdictie van software agenten, (3) transparantie en controleerbaarheid, en (4) de mogelijkheden tot de inper-

king van de gedragingen van software agenten.[1] Deze vragen worden niet beantwoord in het huidige juridisch kader, daar dit kader tot stand is gekomen voor de komst van agenttechnologie.

De eerste en in mijn ogen meest belangrijke kwalitatieve vraag die rijst bij het gebruik van software agenten voor surveillance doeleinden is hun juridische status en kwalificatie als opsporingsbevoegdheid. Software agenten zijn in staat tot intelligent en autonoom handelen, maar de vraag is in hoeverre zij ook bevoegd zijn om zelfstandig opsporingshandelingen uit te voeren.

De tweede vraag heeft betrekking op de jurisdictie van software agenten. Gezien het internationale karakter van het internet, de autonomie van software agenten en hun mobiliteit, is het waarschijnlijk dat zij grensoverschrijdend hun surveillance taken zullen uitvoeren. In dergelijke gevallen is het noodzakelijk om duidelijke afspraken te maken rondom de jurisdictie van software agenten.

De derde vraag die het gebruik van software agenten oproept is naar de transparantie en controleerbaarheid van hun handelen. Omdat agenten grotendeels autonoom handelen zijn hun acties niet altijd voorspelbaar. Het aanpassingsvermogen van agenten en mogelijk emergent gedrag dragen hier verder aan bij. Daarnaast zijn software agenten en agentsystemen complex en kan hun handelen kan daarom moeilijk te doorgronden zijn.

De vierde vraag hangt nauw samen met de eerste en de derde vraag en heeft betrekking op de mogelijkheden om grenzen te stellen aan het handelen van software agenten. Het is noodzakelijk om grenzen te stellen aan het gebruik van software agenten daar zij autonoom kunnen handelen, adaptief kunnen zijn en emergent gedrag kunnen vertonen. Deze eigenschappen stellen agenten in theorie in staat om diverse databases en andere informatiebronnen te benaderen. Om de mogelijkheden van software agenten aan banden te leggen zijn regels noodzakelijk voor hun gebruik. Momenteel ontbreken deze regels.

Uit het voorgaande blijkt dat het juridisch kader voor de bescherming van de privacy en vrijheid door de komst van agenttechnologie aanzienlijk onder druk kan komen te staan door kwantitatieve en kwalitatieve effecten. Het is dus zaak te kijken in hoeverre het juridisch kader voor de bescherming van privacy en vrijheid in de toekomst gestalte dient te krijgen. Hierbij dienen mogelijke aanpassingen aan het juridisch kader mede geëffectueerd te worden in de technologie en de bijbehorende procedures (zie hoofdstuk 9).

Allereerst moet het gebruik en de regulering van software agenten aan een aantal basiselementen voldoen. Deze elementen liggen al expliciet of impliciet besloten in het huidige juridisch kader. Het gaat hier om (1) het strafvorderlijk legaliteitsbeginsel, (2) heldere materieel strafrechtelijke bepalingen, (3) proportionaliteit en subsidiariteit, (4) gelijke behandeling voor de wet,

1 De kracht van de agent metafoor roept in zichzelf geen directe juridische vragen op.

(5) beperkingen aan de bevoegdheden rondom het gebruik van agenten, (6) transparantie en verantwoordelijkheid, en (7) inspraak van de betrokkene(n).

Naast deze algemene vereisten aan het gebruik en de regulering van software agenten moeten met het oog op de kwantitatieve en kwalitatieve effecten van agenttechnologie naar mijn mening enkele specifieke veranderingen worden doorgevoerd.

Het is moeilijk om de kwantitatieve effecten van software agenten te reguleren door middel van wetgeving. De reden hiervoor is dat er geen duidelijk punt is op een schaal waarvan we kunnen zeggen dat het een minimum niveau aan privacy en vrijheid is. Surveillance met behulp van software agenten bevindt zich aldus op een 'hellend vlak'. Er zijn echter wel een aantal mechanismen om de mogelijke negatieve gevolgen van kwantitatieve effecten in te perken. Een eerste mechanisme is het verhogen van het bewustzijn rondom de mogelijke gevolgen van elektronische surveillance voor de (individuele) vrijheid. Een tweede mechanisme is meer aandacht schenken aan de grondrechten die tot op heden te veel op het recht op privacy vertrouwden voor hun bescherming. Hierbij gaat het onder andere op de vrijheid van meningsuiting, het recht op vergadering en het recht op gelijke behandeling. Een derde mechanisme is het implementeren van wet- en regelgeving in de technologie (privacy enhancing technologies en privacy by design). In dit kader is met name de notie van normatieve agenten relevant. Een vierde mechanisme is zeker stellen dat burgers (waar mogelijk) inzage hebben in de surveillance praktijken van de overheid.

Met betrekking tot de kwalitatieve effecten van agenttechnologie is het met name zaak de juridische status van agenten te verduidelijken. Aan de hand van de juridische status van agenten kan vervolgens nadere invulling worden gegeven aan regels omtrent de specifieke eigenschappen van software agenten zoals adaptief vermogen of emergent gedrag en de specifieke juridische vragen die deze eigenschappen oproepen. Met betrekking tot de juridische status van software agenten zijn er vier mogelijkheden: (1) een agent wordt slechts gezien als een instrument, (2) een agent ontleend zijn bevoegdheden aan die van de gebruiker, (3) het gebruik van agenten wordt gezien als een bijzondere opsporingsbevoegdheid, (4) software agenten krijgen een aparte status in de wet. De keuze voor één van deze mogelijkheden is met name afhankelijk van de mogelijke risico's die het gebruik van agenttechnologie meebrengt voor privacy en vrijheid. Hierbij kan gesteld worden dat naarmate agenten een hogere mate van autonomie hebben en intelligenter zijn, de risico's toenemen. Het ligt dus voor de hand om de keuze voor een juridische status tot op zekere hoogte gelijk te schakelen met de ontwikkeling van agenttechnologie. Uitgangspunt hierbij is dat naarmate agenten intelligenter worden hun gedrag meer gereguleerd moet worden en het dus voor de hand ligt om een 'zwaardere' juridische status toe te kennen aan software agenten.

We kunnen concluderen dat software agenten de surveillance effectiever en efficiënter maken, een ontwikkeling die de privacy en vrijheid van de

geobserveerden onder druk zet. Door de inrichting van een omvangrijke surveillance infrastructuur en de daarmee gepaard gaande panoptische gevoelens zal met name de positieve vrijheid onder druk komen te staan, daar waar voorheen het met name de negatieve vrijheid was die in het gedrang was. Voorts kunnen we concluderen dat het huidige juridisch kader voor de bescherming van de privacy en de vrijheid, dat met name geconcentreerd is rond het privacybegrip, in de toekomst niet langer afdoende zal blijken. Toch ben ik van mening dat met de voorgestelde aanpassingen aan het juridisch kader de kwantitatieve effecten en kwalitatieve effecten van agenttechnologie afdoende geadresseerd kunnen worden.

References

Aarts, E., Harwig, R., Schuurmans, M. (2002). *Ambient Intelligence*, in: Denning, P.J. (ed.), *The Invisible Future: The Seamless Integration of Technology in Everyday Life*, pp. 235-250. New York: McGraw Hill

Agre, P.E. (2001), Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places, in: *Whole Earth* 106, Winter 2001, p. 74-77

Ahola, J. (2001). Ambient Intelligence, in: *ERCIM News*, No. 47, October 2001

AIVD (2004). *Van Dawa tot Jihad: de Diverse Dreigingen van de Radicale Islam Tegen de Democratische Rechtsorde*. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (in Dutch)

Aristotle (350 BC). *The Politics* and *The Constitution of Athens*, republished in 1995 (ed. Everson, S.), Cambridge: Cambridge University Press

Bacon, F. (1597). *Mediationes Sacrae, de Haeresibus*

Bacon, F. (1620). *Novum Organum Scientiarum*

Bailey, D. (2004). *The Open Society Paradox: Why the 21st Century Calls for More Openness, Not Less*, Washington: Potomac Books

Baird, Z., Barksdale, J., Vatis M.A. (2003). *Creating a Trusted Information Network for Homeland Security: Second Report of the Markle Foundation Task Force on National Security in the Information Age*. Markle Foundation, December 2003

Bazan, E.A. (2004). *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions*, CRS Report for Congress

Bentham, J. (1843). *Jeremy Bentham: Collected Works* (ed. Browning, J.), London

Berlin, I. (1958). *Two concepts of Liberty*, republished in 2002 as: *Liberty* (ed. Hardy H.), Oxford: Oxford University Press

Blok, P. (2002). *Het Recht op Privacy*, Den Haag: Boom Juridische uitgevers (in Dutch)

Bloustein, E.J. (1984). Privacy as an Aspect of Human Dignity: an Answer to Dean Prosser, in: F.D. Schoeman (ed.), *Philosophical Dimensions of Privacy: an Anthology*, New York: CUP, p. 156-202

Bor, J., Petersma, E. (2000). *De verbeelding van het denken: Geïllustreerde geschiedenis van de westerse en oosterse filosofie,* Amsterdam: Uitgeverij Contact (in Dutch)

Borking, J., Artz, M., van Almelo, L. (1998). *Gouden Bergen van Gegevens: Over Datawarehousing, Data mining en Privacy, Achtergrondstudies en Verkenningen nr. 11*, Den Haag: Registratiekamer (in Dutch)

Borking, J., van Eck, B.M.A., Siepel P. (1999). *Intelligent Software Agents and Privacy, Achtergrondstudies en Verkenningen nr. 13*, Den Haag: Registratiekamer. (in Dutch)

Bovens, M.A.P. (1998). *De Digitale Rechtsstaat, beschouwingen over informatiemaatschappij en Rechtsstaat* (in Dutch)

Bradshaw, J. (1998). *Software Agents*, Menlo Park, California: AAArtificial-intelligence Press

Brazier, F.M.T., Kubbe, O., Oskamp, A., Wijngaards, N.J.E. (2002). Are Law-Abiding Agents Realistic?, in: *Proceedings of the workshop on the Law of Electronic Agents (LEA02)*, July 2002

Brazier, F., Oskamp, A., Prins, J.E.J., Schellekens, M.H.M., Wijngaards, N.J.E., Apistola, M., Voulon, M., Kubbe, O (2003). *Analysing Legal Implications and Agent Information Systems*, Technical Report No. IR CS 004, Amsterdam, Vrije Universiteit

Brenner, W., Zarnekow, R., Wittig, H. (1998). *Intelligent Agents: Foundations and Applications*, Berlin: Springer Verlag.

Brin, D. (1999). *The Transparent Society*, Redding: Perseus Books

Brooks, R.A. (1991a), Intelligence without representation, in: *Artificial-intelligence*, 47, p. 139-159

Brooks, R.A. (1991b), How to build complete creatures rather than isolated cognitive simulators, in: *Architectures for Intelligence* (ed. VanLehn, K.), pp. 225-239, Hillsdale, NJ: Lawrence Erlbaum Assosiates. (PDF version)

Brouwer, D.V.A. (2000). Het verkennend onderzoek in strafzaken en de wetgevingsspiraal, in: *Nederlands Juristenblad*, 2000, p. 637-640 (in Dutch)

Brown, D., Wiggers, E. (2005). *Planning for Proliferation: The Impact of RFID on the Network*, IDC Whitepaper March 2005

Carter, I. (2003). Positive and Negative Liberty, in: *The Stanford Encyclopedia of Philosophy* (Spring 2003 Edition), ed. Edward N. Zalta.

Castelfranchi, C., Dignum, F., Jonker, J.M., Treur, J. (1999). Deliberative Normative Agents: Principles and Architecture, in: *Lecture Notes In Computer Science*; Vol. 1757; 6th International Workshop on Intelligent Agents, Agent Theories, Architectures, and Languages (ATAL) 1999, Pages: 364-378, London: Springer Verlag 1999

Choi, Y.S., Yoo, S.I., Lee, J. (1999). *Neural Network Based Multi-agent Information Retrieval System*.

Christman, J. (1991). Liberalism and Individual Positive Freedom, in: *Ethics*, 1001, p. 343-359.

Clarke, R. (1994). The Digital Persona and its Application to Data Surveillance, in: *The Information Society*, June 10-2.

Cleiren, C.P.M. (2006). 'Aanwijzingen' voor de wetgeving bij veiligheidsvraagstukken en terrorismebestrijding, in: *Veiligheid en Recht, Nieuwe Doelwitten en Strategieën* (eds. Huisman, W., Moerings, L.M., Suurmond, G.) Den Haag: Boom Juridische uitgevers (in Dutch)

Cohen, J.E. (2000). Examined Lives: Informational Privacy and the Subject as Object, in: *Stanford Law Review*, vol. 52: 1373 May 2000, p. 1373-1437.

Cohen, J.E (2003). Symposium, the Law and Technology of Digital Rights Management: DRM and Privacy, in: *Berkley Technology Law Journal* 18, 575, 609-617.

Cohen, S. (1985). *Visions of Social Control*, Cambridge: Polity Press

DARPA (2003). *Report to Congress regarding the Terrorism Information Awareness Program*,

Dartel, van, M. (2005). Situated Representation, SIKS Disseration Series No. 2005-19, Maastricht: Universiteit Maastricht

Das, S.,Wu,C., Truszkowski, W. (2001) Distributed Intelligent Planning and Scheduling for Enhanced Spacecraft Autonomy, in: *Proceedings of the 2001 AAAI Spring Symposium Series, Palo Alto, CA* (March).

DeLeuze, G., Guattari, F. (1987), *A Thousand Plateaus*, Minneapolis: University of Minnesota Press

DeLeuze, G. (1992). Postscripts on the Societies of Control, in: *OCTOBER 59*, Winter 1992, MIT Press, Cambridge, MA, pp. 3-7

Department of Justice (2002), *The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations*.

De Miglio, F. Onida, T. Romano, F., Santoro, S. (2002). *Electronic Agents and the Law of Agency*. LEA 2002, Workshop on the Law of Electronic Agents, July 13, 2002

Dick, P.K. (1956). *The Minority Report*, republished in 2002, New York: Kensington Publishing Corporation

Dubbeld, L. (2004). *The Regulation of the Observing Gaze: Privacy Implications of Camera Surveillance*, Enschede: Ipskamp Printpartners

Dutch Data Protection Authority (2004). *Annual Report 2003*, Den Haag: Deltahage BV

Doyle, S. (2002). *The USA Patriot Act: a Legal Analysis*, CRS Report for Congress, order code CRL31377

Dworkin, R. (1986). *Law's Empire*, Cambridge: Harvard University Press

Dyer, D. (2002), *Genisys*, speech at DARPATECH 2002

Edwards, S.J.A. (1999). *Swarming on the Battlefield: Past, Present, and Future*. RAND MR-1100-OSD

Etzioni, A. (1999). *The Limits of Privacy*, New York: Basic Books

Etzioni, O., Weld, D.S. (1995). Intelligent Agents on the Internet: Fact, Fiction and Forecast, in: *IEEE Expert* 10(3), p. 44-49

Fayyad, U., Piatetsky-Shapiro, G., Smyth, P. (1996). From data mining to knowledge discovery in databases (a survey), in: *AI Magazine*, 17(3), pages 37-54, 1996

Feenberg, A. (2000). From Essentialism to Constructivism: Philosophy of Technology at the Crossroads, in: *Technology and the Good Life* (eds. Higgs, E., Strong, D., and Light, A.). Chicago: University of Chicago Press, 2000, pp. 294-31

Filmer, R. (1680). *Patriarcha and Other Political Writings,* republished in 1949 (ed. Laslett, P.), Oxford: Blackwell Publishers Limited

Finin, T., McKay. D., Fritzson, R. (1992). An overview of KQML: A Knowledge Query and Manipulation Language. The KQML Advisory Group, March 2, 1992

Foley, R.K. (1978). The Problem with Power, *The Freeman*, March 1978, Vol. 28, No. 3

Foucault, M. (1975). *Discipline and Punish, the Birth of the Prison*, republished in 1995, New York: Vintage Books

Foucault, M. (1997). *The Politics of Truth* (ed. Sylvère Lotringer), Semiotext(e)

Franken, H. (1995). *In*leiden *tot de rechtswetenschap*. Arnhem: Gouda Quint (in Dutch)

Franken, H., Arnbak, J., Bovens, M.A.P., Donner, J.P.H, Gerritsma, A.M., Kummeling, H.R.B.M., Prins, J.E.J., de Ru, H.J., Snellen, I.Th.M., Vogelzang, P. (2000). *Rapport van de Commissie Grondrechten in het Digitale Tijdperk*. Rotterdam: Phoenix & Den Oudsten. (in Dutch)

Franken, H., Prins, J.E.J., van Esch, R.E., Quaedvlieg, A.A., Dommering, E.J., Koers, A. W. Koers, Schmidt, A.H.J., Lips, A.M.B. (2003). *Zeven Essays over Informatietechnologie en Recht,* Den Haag: Sdu Uitgevers (in Dutch)

Franken, H., Kaspersen H.W.K., de Wild, A.H. (2004). Recht en Computer (Fifth Edition). Deventer: Kluwer (in Dutch)

Franklin, S., Graesser A. (1996). Is It an Agent or Just a Program? A taxonomy for Autonomous Agents, in: *Proceedings of the Third International Workshop on Agent Theories, Architectures and Languages*. New York: Springer Verlag.

Frawley, W.J. Piatetsky-Shapiro, G., Matheus, C.J. (1992). Knowledge Discovery in Databases: An Overview, in: *AAAI Magazine*, Fall 1992

Fuller, L.L. (1964). *The Morality of Law*, revised edition, New Haven: Yale University Press

Gandy, O. (1993). *The Panoptic Sort: A Political Economy of Personal Information*, Boulder: Westview Press

Gandy, O. (1996). Coming to terms with the Panoptic Sort, in: *Computers, Surveillance and Privacy* (eds. Lyon, D., Zureik, E.), Minneapolis: University of Minnesota Press

Gartska, J.J. (2003) Network-Centric Warfare Offers Warfighting Advantage, in: *Signal,* May 2003

Gaus, G., Courtland, S.D. (1997). Liberalism, in: *The Stanford Encyclopedia of Philosophy* (ed. Edward N. Zalta).

Gilbert, D. *et al.* (1995). *IBM Intelligent Agent Strategy*, IBM Corporation

Gilliom, J. (2001). *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy*, Chicago: The University of Chicago Press

Ginsberg M. (1989). Universal planning: An (almost) universally bad idea. *Artificial-intelligence Magazine* 10(4):40-44

Goffman, E. (1959), *The Presentation of Self in Everyday Life*, New York: Doubleday

Government Accountability Office (2004), *Data Mining: Federal Efforts Cover a Wide Range of Uses,* GAO Report 04-548

Graham, B., *et al.* (2002). Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001. S. Rept. No. 107- 351 107th Congress, 2D Session H. Rept. No. 107-792

Gill, M., Spriggs, A. (2005). *Assessing the Impact of CCTV*, Home Office Research Study 292

Gutwirth, S. (1998). *Privacyvrijheid! De vrijheid om zichzelf te zijn,* Amsterdam: Otto Cramwinckel Uitgevers. (In Dutch)

Haggerty, K.D., Ericson, R.V. (2000). The Surveillant Assemblage, in: *The British Journal of Sociology*, Vol. 51 Issue 4 605 December 2000, p. 605-622

Hampsher-Monk, I. (1992). *A History of Modern Political Thought*, Oxford: Blackwell Publishers Limited.

Hart, H.L.A. (1961). *The Concept of Law*, (Second Edition) Oxford: Clarendon Press 1994

Heidegger, M. (1953). *Die Frage nach der Technik*, Vorträge und Aufsätze, Pfullingen: Neske, 1954

Heidegger, M. (1977). *The Question Concerning Technology and Other Essays*, W. Lovitt (trans) New York: Harper and Row

Heidegger M. (2002). *Alleen nog een God kan ons redden, Heidegger in gesprek met Der Spiegel*, Kampen: Klement/Pelckmans (in Dutch)

Herik, H.J. van den (1983). *Computerschaak, Schaakwereld en Kunstmatige Intelligentie*. Proefschrift TH Delft. 's-Gravenhage: Academic Service (in Dutch)

Herik, H.J. van den (1991). *Kunnen Computers* Rechts*preken?*, Inaugurele reden Leiden, Arnhem: Gouda Quint (in Dutch)

Herik, H.J. van den, Wiesman, F., Roos, N. (2001). *Internal Report Infonomics*, IKAT, Universiteit Maastricht

Herik, H. J. van den, Schermer, B. W. (2006). Elektronische Surveillance, Veiligheid en Privacy, in: *Veiligheid en Recht, Nieuwe Doelwitten en Strategieën* (eds. Huisman, W., Moerings, L. M., Suurmond, G.) Den Haag: Boom Juridische uitgevers (in Dutch)

Hoecke, van, M. (2002). *Law as Communication*. Oxford and Portland, Oregon: Hart Publishing

Hoven, van den, J. (1999). Privacy and the Varieties of Informational Wrongdoing, in: *Australian Journal of Professional and Applied Ethics*, Special Issue, vol. 1, June 1999

Hustinx, P. J. (2004). Bescherming van Persoonsgegevens op Koers, in: *Rechtsgeleerd Magazijn THEMIS*, 2004 no. 5 (in Dutch)

Innes, M. (2003). *Understanding Social Control: Deviance, Crime and Social Order*, Berkshire: Open University Press

Jennings, N.R., Wooldridge, W.J. (1998), *Agent Technology, Foundations, Applications and Markets*, Berlin: Springer Verlag

Kant, I.M. (1784). Beantwortung der Frage: Was ist Aufklärung?, republished in: *Schriften zur Antropologie, Geschichtsphilosophie, Politik und Pädagogik*, (ed. Weischedel, I.W.) 1981, Suhrkamp: Frankfurt am Mein, p. 53-61 (in German)

Kean, T.H. *et al.* (2004), *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks on the United States*, official government edition, US Government Printing Office

Kemal, D.A., Dayal, U. (2006). AI Re-Emerging as Research in Complex Systems, in: *Ubiquity*, Volume 7, Issue 38

Kerr, O.S. (2004). The Fourth Amendment and New Technologies: Constitutional Myths and a Case for Caution, George Washington University Law School, public research paper nr. 66

Knowledge Computing Corporation (2004). *The COPLINK Whitepaper*, 2004/3

Koelewijn W.I., Kielman, H. H. (2006). Agenten voor Agenten: Slimme Software ter Ondersteuning van Menselijk Handelen, in: *Veiligheid en Recht, Nieuwe Doelwitten en Strategieën* (eds. Huisman, W., Moerings, L.M., Suurmond, G.) Den Haag: Boom Juridische uitgevers (in Dutch)

Kolkman, P., van Kralingen, R., Nouwt, S. (2000). *Privacy in Bits en Bytes, privacyaspecten van electroninc monitoring in netwerkomgevingen*, Den Haag: Sdu Uitgevers (ITeR Reeks nr. 38) (in Dutch)

Koops, B.J., Vedder, A.H. (2001), *Opsporing versus privacy: de beleving van burgers*, ITeR-deel 45, Den Haag: Sdu Uitgevers 2001 (ITeR Reeks nr. 45) (in Dutch)

Koops B.J. (2004), *Strafrecht en ICT* (Monografieën Recht en Informatietechnologie Deel 1), Den Haag: Sdu (in Dutch)

Krikke, J. (2006) Intelligent Surveillance Empowers Security Analysts, in: *IEEE Intelligent Systems*, May/June issue 2006

Kurzweil, R. (1990), *The Age of Intelligent Machines*, Cambridge MA: MIT Press

Kurzweil, R (1999), *The Age of Spiritual Machines*, New York: Penguin

Kurzweil, R. (2005), *The Singularity is Near, When Humans Transcend Biology*, New York: Viking

Kymlicka, W. (1990). *Contemporary political philosophy: an introduction*, Oxford: Clarendon Press

Langheinrich, M. (2001). Privacy by Design – Principles of Privacy Aware Ubiquitous Systems, in: *Proceedings of Ubicomp 2001*, pp. 273-291, Springer-Verlag LNCS 2201, 2001

Lessig, L. (1999). *Code and Other Laws of Cyberspace,* New York: Basic Books

Locke, J. (1690). *The Second Treatise of Government and a Letter Concerning Toleration,* republished in 1981 (ed. Gough, J.W.), New York: Dover Publications

Luck, M., McBurney, P., Preist, C. (2003), *Agent Technology: Enabling Next Generation Computing. A Roadmap for Agent-Based Computing*. AgentLink II, IST-1999-29003

Luck, M., Ashri R., D'Iverno M. (2004), *Agent-based Software Development*, Norwoord: ArtechHouse Inc.

Lyon, D. (1994). *The Electronic Eye, the Rise of Surveillance Society*, Minneapolis: University of Minnesota Press

Lyon, D., Zureik, E. (1996). *Computers, Surveillance, and Privacy*, Minneapolis: University of Minnesota Press

Lyon, D. (2001). *Surveillance Society, Monitoring everyday life*, Buckingham: Open University Press

Lyon, D. (2003a). *Surveillance as Social Sorting, Privacy, Risk and Digital Discrimination*, New York: Routledge

Lyon, D. (2003b). *Surveillance after September 11*, Cambridge: Polity Press

MacCallum, G. C. (1967). Negative and positive freedom, *Philisophical Review*, 76, p. 312-334

Maes, P. (1995a). Modeling Adaptive Autonomous Agents, in: *Knowledge Engineering Review*

Maes, P. (1995b). Artificial Life Meets Entertainment: Life like Autonomous Agents, in: *Communications of the ACM*, 38, 11, 108-114

Marx, G.T. (1985). The surveillance society: the threat of 1984-style techniques, *The Futurist*, June 21-6

Marx, G.T. (2001). Murky conceptual waters: the public and the private, in: *Ethics and Information Technology*, 2001. vol 3, no. 3, p. 157-16

Mathiesen, T. (1997). The Viewer Society: Michael Foucault's Panopticon Revisited, in: *Theoretical Criminology*, 1 (2), p. 215-234

McCahill, M., Norris, C. (2002). *CCTV in Britain*. Working Paper nr. 3 of the Urban Eye Project, 5th framework programme of the European Commission, contract number: HPSE-CT2001-00094

McCarthy, J., Hayes P.J. (1969), Some Philosophical Problems from the Standpoint of Artificial-intelligence, in: *Machine Intelligence*, 4

McClellan, J.S. (1996). *A History of Western Political Thought*, London: Routledge

Ména, J. (2004). *Homeland Security: Techniques and Technologies*, Charles River Media: Hingham, MA

Michaels, C.W. (2002). *No greater threat: America after September 11 and the rise of a national security state*, New York: Algora Publishing

Mill, J.S. (1859). *Utilitarianism and On Liberty*, republished in 2003 (ed. Warnock, M.), Malden: Blackwell Publishing

Minow, *et al.* (2004). *Safeguarding Privacy in the Fight Against Terrorism: Report of the Technology and Privacy Advisory Committee*, March 2004.
Minsky M. (1986). *The Society of Mind*, New York: Simon and Schuster
Moerings, L.M., (2006). *Risicojustitie als inzet voor een veiliger samenleving*, in: in: *Veiligheid en Recht, Nieuwe Doelwitten en Strategieën* (eds. Huisman, W., Moerings, L.M., Suurmond, G.) Den Haag: Boom Juridische uitgevers (in Dutch)
Mohammadian, M., Jentzsch, R. (2004). Computational Intelligence Techniques Driven Intelligent Agents for web Data Mining and Information Retrieval, in: *Intelligent Agents for Data Mining and Information Retrieval* (ed. Mohammadian, M.), London: Idea Group Publishing
Mumford, L. (1934). *Technics and Civilization*, Orlanda: Harcourt & Brace
Mutton, P. (2004). *Inferring and Visualizing Social Networks on Internet Relay Chat*. Information Visualisation Conference July 2004

Norris, C., Armstrong G. (1999), *The Maximum Surveillance Society: The rise of CCTV*, Oxford: Berg
Negroponte, N. (1995). *Digitaal Leven*, Amsterdam: Ooievaar (in Dutch)
Nieuwenhuis, A.J. (2001). *Tussen privacy en persoonlijkheidsrecht, een grondrechtelijk en rechtsvergelijkend onderzoek,* Nijmegen: Ars Aequi Libri (in Dutch)
Nieuwenhuis, H.J. (2003). Hellend Vlak. Kelly en de Claimcultuur, in: *NJB* 2003, p. 1380-1382 (in Dutch)
Nwana, S. (1996). Software Agents: An Overview, in: *Knowledge Engineering Review,* (11) 3 (PDF version)

Odlyzko, A.M. (2003). Privacy, Economics, and Price discrimination on the Internet, *ICEC2003: Fifth International Conference on Electronic Commerce*, (ed. N. Sadeh) ACM, 2003, pp. 355-366.
Office of Technology Assessment (1988). *Criminal Justice: New Technologies and the Constitution, a Special Report*, Washington, DC: Government Printing Office
Orwell, G. (1949). *Nineteen eighty-four*, London: Penguin Books

Parent W.A. (1983). Privacy, Morality, and the Law, *Philosophy and Public Affairs*, vol. 12, no. 4 pp. 269-88
Parenti, C. (2003). *The Soft Cage: Surveillance in America, From Slave Passes to the War on Terror,* New York: Basic Books
Patton, P. (1994). Metamorphologic: Bodies and Powers in a Thousand Plateaus, in: *Journal of the British Society for Phenomenology* 25 (2) p. 157-169
Peissl, W. (2002). Surveillance and Security: a Dodgy Relationship, in: *Debating Privacy and ICT Before and After September11th, conference papers of the International Conference on the use of personal data in criminal investigations and commerce,* January 17th 2002
Phillips, L.R., Link, H.E., Goldsmith, S.Y. (2002). *Agent-Based Mediation and Cooperative Information Systems,* SAND Report 2002-1760 Sandia National Labratories
Poster, M. (1990). *The Mode of Information*, Cambridge: Polity Press
Postma, E.O. (2003), *De Onderste Steen Boven*, Oratie Universiteit Maastricht (in Dutch)
Prins, J.E.J., (2003). Acht gesprekken over privacy en aanpalende belangen, in: Franken *et al.* (2003), *Zeven Essays over Informatietechnologie en recht,* Den Haag: Sdu Uitgevers (in Dutch)

Qi, H., Wang, X., Sitharama Iyengar, S., Chakrabarty, K. (2001). *Multisensor Data Fusion in Distributed Sensor Networks Using Mobile Agents*, Duke University

Rao, A.S., Georgeff, M.P. (1995). BDI Agents: From Theory to Practice, in: *Proceedings of the First International Conference on Multi-Agent Systems (ICMAS-1995)*, San Francisco, June 1995

Rawls, J. (1971). *A Theory of Justice* (Revised Edition), Oxford: Oxford Univeristy Press 1999

Read, S. (1995). *Thinking About Logic. An Introduction to the Philosophy of Logic*. Oxford: Oxford University Press

Rhodes, J., Maes, P. (2000). Just In Time Information Retrieval Agents, in: *IBM Systems Journal*, Vol. 39, NOS 3&4

Rosen, J. (2000). *The Unwanted Gaze: the Destruction of Privacy in the United States*, New York: Vintage Books

Rosen, J. (2004). *The Naked Crowd, Reclaiming Security and Freedom in an Anxious Age*, New York: Random House

Rosenzweig, P. (2003). *Proposals for Implementing the Terrorism Awareness Information System*, Legal Memorandum no. 8, August 2003, the Heritage Foundation

Rotenberg, M. (2003). *The Privacy Law Sourcebook 2003*, Washington: Electronic Privacy Information Center.

Russell, S.J., Norvig, P. (1995). *Artificial-intelligence: A Modern Approach*, Englewood Cliffs, NJ: Prentice Hall

Sawyer, M. (2003). Connecting the dots: the challenge of improving the creation and sharing of knowledge about terrorists, in: *Journal of Homeland Security*

Schafer, B., Rodriguez-Rico, M., VandenBerghe, W. (2004). Undercover Agents and Agents Provocateur; Evidence Collection by Autonomous Agents and the Law, in: *Proceedings of the workshop on the Law of Electronic Agents (LEA04),* July 2004

Schermer, B.W., Durinck, M., Bijmans, L. (2005). *Juridische Aspecten van Autonome Systemen*, Leidschendam: ECP.NL (in Dutch)

Schmalleger, F. (2005). Criminal Justice Today, an Introductory Text for the 21st Century (eighth edition), New Jersey: Pearson Prentice Hall

Sena, J.A. (2000). Collaborative Decision Support System for Navy Pier and Port Management, *Crosstalk, The Journal for Defense Software Engineering*, February 2000

Senator, T. (2002). *Evidence Extraction and Link Discovery Program*, speech at DARPATech 2002

Sennett, R. (1990), *The Conscience of the Eye.* New York: W.W. Norton.

Seydim, A.Y. (1999). *Intelligent Agents: a Data Mining Perspective.* Department of Computer science and Engineering, Southern Methodist University (PDF version)

Shannon, C. (1950). Programming a Computer for Playing Chess. *Philosophical Magazine*, 41

Shoham, Y. (1997). An Overview of Agent-oriented Programming. In *Software Agents*, ed. J. M. Bradshaw. Menlo Park, California.: AAArtificial-intelligence Press

Seifert, W. (2006). *Datamining and Homeland Security: An overview*. Report for Congress RL31798, January 27 2006

Sietsma, R., Verbeek, J., Van den Herik, J., (2002). *Data mining en Opsporing*, Den Haag: Sdu Uitgevers (ITeR Reeks nr. 55) (in Dutch)

Skinner, Q. (1998). *Liberty before Liberalism*, Cambridge: Cambridge University Press

Solove, D.J. (2001). Privacy and Power: Computer Databases and Metaphors for Information Privacy, in: *Stanford Law Review*, vol. 53, pp. 1393
Solove, D.J. (2002a). Conceptualizing Privacy, in: *California Law Review*, vol. 90, pp. 1087
Solove, D.J. (2002b). Digital Dossiers and the Dissipation of Fourth Amendment Privacy, in: *Southern California Law Review*, Vol. 75, July 2002
Solove, D.J. (2004a), Reconstructing Electronic Surveillance Law, in: *George Washington Law Review*, Vol. 72
Solove, D.J. (2004b), *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press
Solum, L.B. (1992), Legal Personhood for Artificial Intelligences, *North Carolina Law Review*, 2, 1231
Stalder, F. (2003). Privacy is not the antidote to surveillance, in: *Surveillance and Society 1 (1)*
Stanley, J., Steinhardt, B. (2003). *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, New York: ACLU
Staples, W.G. (2000), *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, Oxford: Rowman & Littlefield Publishers
Stewart, I., Cohen, J. (1999). *Figments of Reality*, Cambridge: Cambridge University Press
Stone, P., Veloso, M. (1997). *Multi-agent Systems: A Survey from a Machine Learning Perspective*. Pittsburgh: Carnegie Mellon University
Strat, T.M., Welby, S.P. (2004). *Proposer Information Pamphlet, Combat Zones that See*. DARPA
Stuurman, C., Wijnands, H. (2000). *Intelligent Agents: Vloek of Zegen?*, in: *de e-consument, consumentenbescherming in de nieuwe economie*, Den Haag: Elsevier Juridisch (in Dutch)
Sunstein, C.R. (2001). *Republic.com*, New Jersey: Princeton University Press
Soans, C., Stevenson, A. (2004). *The Concise Oxford Dictionary of Current English*, eleventh edition, Oxford: Oxford University Press

Taipale, K.A. (2003). Data mining and Domestic Security: Connecting the Dots to Make Sense of Data, in: *The Columbia Science and Technology Law Review*, Vol. V 2003
Taipale, K.A. (2004). Technology, Security and Privacy: the Fear of Frankenstein,the Mythology of Privacy and the lessons of King Ludd, in: *International Journal of Communications Law & Policy*, special issue on cybercrime, winter 2004/2005
Taylor, C. (1979). *Hegel and Modern Society*, Cambridge: Cambridge University Press.
Taylor, N. (2003). State Surveillance and the Right to Privacy, in: *Surveillance & Society 1 (1)*
Terstegge, J.H.J. (2006). Toepassingen en Toekomst van RFID, in: *Privacy en Andere Juridische Aspecten van RFID* (eds. Zwenne, G.J., Schermer, B.W.), Den Haag: Elsevier Juridisch (in Dutch)
Thomson, J.J. (1975). The Right to Privacy, in: *Philosophy and Public affairs*, p. 295-315
Turing, A. (1950). Computing Machinery and Intelligence, in: *Mind*, 59 4333-460
Turban, E. (1995). *Decision Support and Expert Systems: Management Support Systems*. Englewood Cliffs, N.J., Prentice Hall
Two Crows Corportation (1999). *Introduction to Data Mining and Knowledge Discovery 3rd edition,* Potomac MD: Two Crows Corp.

Verbeek, J., Van den Herik, H.J., Plugge, L., de Roos, T. (1999). *Politie en Intranet*, Deventer: Kluwer 1999 (ITeR Reeks nr. 19) (in Dutch)

Verheij, B. (1996). *Rules, Reasons, Arguments. Formal Studies of Argumentation and Defeat*. Universiteit Maastricht
Vlassis, N. (2003). *A Concise Introduction to Mulitagent Systems and Distributed Artificial-intelligence*, Amsterdam: University of Amsterdam

Wagner DeCew, J. (1997). *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*, Ithaca: Cornell University Press.
Wahdan, M. (2006). *Automatic formulation of the Auditor's Opinion*, SIKS Dissertation Series 2006-09
Warren S.D., Brandeis L.D. (1890). The Right to Privacy: the Implicit Made Explicit, in: *Harvard Law Review*, p. 193-220
Wawro G. (2000). *Warfare and Society in Europe 1792-1914,* London: Routledge
Wechsler, D. (1958). *The Measurement and Appraisal of Adult Intelligence*. Baltimore, MD: The Williams & Wilkins Company
Westin, A.F. (1967). *Privacy and Freedom*, New York: Atheneum Press
Westin, A.F. (1984). The Origins of Modern Claims to Privacy, in: *Philosophical Dimensions of Privacy: an Anthology* (ed. Schoeman, F. D.), Cambridge: Cambridge University Press, p. 56-74
Wexelblat, A. (2001). How is the National Information Infrastructure Like a Prison?, in: *True Names and the Opening of the Cyberspace Frontier* (ed. Frenkel, J.), New York: Tom Doherty Associates
Wooldridge, M. (2002), *An Introduction to Multi-agent Systems*, West Sussex: John Wiley & Sons Ltd.
Wooldridge, M., Jennings, N.R. (1995). *Intelligent Agents: Theory and Practice,* Knowledge Engineering Review

Yang, J., Honavar, V., Miller, L., Wong, J. (1998). *Intelligent Mobile Agents for Information Retrieval and Knowledge Discovery from Distributed Data and Knowledge Sources*

Zandzee, C.G. (1998). *Doelbewust volgen: Privacy Apsecten van cliëntvolgsystemen en andere vormen van gegevensuitwisseling*, Achtergrondstudies en Verkenningen nr. 9, Den Haag: Registratiekamer (in Dutch)
Zwenne, G.J. (2003). Boekbeschouwing, Peter Blok, Het Recht op Privacy, in: *RM Themis* 2003/6 (in Dutch)

FIPA SPECIFICATIONS:

FIPA (2001). *FIPA Personal Assistant Specification*. Document number: XC00083B <http://www.fipa.org>
FIPA (2002a). *FIPA Abstract Architecture Specification*. Document number: SC00001L <http://www.fipa.org>
FIPA (2002b). *FIPA Agent Management Specification*. Document number: SC00023J <http://www.fipa.org>
FIPA (2002c). *FIPA ACL Message Structure Specification*. Document number: SC00061G <http://www.fipa.org>

FIPA (2002d). *FIPA Communicative Act Library Specification*. Document number: SC000037J
<http://www.fipa.org>
FIPA (2002e). *FIPA Message Transport Service Specification*. Document number: SC000067F
<http://www.fipa.org>

Curriculum vitae

Bart Willem Schermer was born in Alkmaar on July 1, 1978. He studied law (IT law and criminal law) at Leiden University. For his Master Thesis, he received the ITeR best thesis award. In 2001, Bart started working as a legal consultant for ECP.NL, the Platform for eNetherlands. In his professional work he focusses on privacy, surveillance, online gaming, and ambient intelligence.

Bart has conducted his Ph.D. research at eLaw@Leiden, Centre for Law in the Information Society, and the E.M. Meijers Institute of Legal Studies. Via his supervisor, Jaap van den Herik, he was also affiliated with SIKS, the Dutch Research School for Information and Knowledge Systems. Bart will continue to work for eLaw@Leiden as a researcher.

SIKS DISSERTATION SERIES

1998

01 Johan van den Akker (CWI) *DEGAS – An Active, Temporal Database of Autonomous Objects*
02 Floris Wiesman (UM) *Information Retrieval by Graphically Browsing Meta-Information*
03 Ans Steuten (TUD) *A Contribution to the Linguistic Analysis of Business Conversations within the Language/Action Perspective*
04 Dennis Breuker (UM) *Memory versus Search in Games*
05 E.W.Oskamp (RUL) *Computerondersteuning bij Straftoemeting*

1999

01 Mark Sloof (VU) *Physiology of Quality Change Modelling; Automated modelling of Quality Change of Agricultural Products*
02 Rob Potharst (EUR) *Classification using decision trees and neural nets*
03 Don Beal (UM) *The Nature of Minimax Search*
04 Jacques Penders (UM) *The practical Art of Moving Physical Objects*
05 Aldo de Moor (KUB) *Empowering Communities: A Method for the Legitimate User – Driven Specification of Network Information Systems*
06 Niek J.E. Wijngaards (VU) *Re-design of compositional systems*
07 David Spelt (UT) *Verification support for object database design*
08 Jacques H.J. Lenting (UM) *Informed Gambling: Conception and Analysis of a Multi-Agent Mechanism for Discrete Reallocation*

2000

01 Frank Niessink (VU) *Perspectives on Improving Software Maintenance*
02 Koen Holtman (TUE) *Prototyping of CMS Storage Management*
03 Carolien M.T. Metselaar (UvA) *Sociaal-organisatorische gevolgen van kennistechnologie; een procesbenadering en actorperspectief*
04 Geert de Haan (VU) *ETAG, A Formal Model of Competence Knowledge for User Interface Design*
05 Ruud van der Pol (UM) *Knowledge-based Query Formulation in Information Retrieval*
06 Rogier van Eijk (UU) *Programming Languages for Agent Communication*
07 Niels Peek (UU) *Decision-theoretic Planning of Clinical Patient Management*
08 Veerle Coup ìe (EUR) *Sensitivity Analyis of Decision-Theoretic Networks*
09 Florian Waas (CWI) *Principles of Probabilistic Query Optimization*
10 Niels Nes (CWI) *Image Database Management System Design Considerations, Algorithms and Architecture*
11 Jonas Karlsson (CWI) *Scalable Distributed Data Structures for Database Management*

2001

01 Silja Renooij (UU) *Qualitative Approaches to Quantifying Probabilistic Networks*
02 Koen Hindriks (UU) *Agent Programming Languages: Programming with Mental Models*
03 Maarten van Someren (UvA) *Learning as problem solving*
04 Evgueni Smirnov (UM) *Conjunctive and Disjunctive Version Spaces with Instance-Based Boundary Sets*
05 Jacco van Ossenbruggen (VU) *Processing Structured Hypermedia: A Matter of Style*
06 Martijn van Welie (VU) *Task-based User Interface Design*
07 Bastiaan Schonhage (VU) *Diva: Architectural Perspectives on Information Visualization*
08 Pascal van Eck (VU) *A Compositional Semantic Structure for Multi-Agent Systems Dynamics*
09 Pieter Jan 't Hoen (RUL) *Towards Distributed Development of Large Object-Oriented Models, Views of Packages as Classes*

10 Maarten Sierhuis (UvA) *Modeling and Simulating Work Practice BRAHMS: a multiagent modeling and simulation language for work practice analysis and design*
11 Tom M. van Engers (VU) *Knowledge Management: The Role of Mental Models in Business Systems Design*

2002

01 Nico Lassing (VU) *Architecture-Level Modifiability Analysis*
02 Roelof van Zwol (UT) *Modelling and searching web-based document collections*
03 Henk Ernst Blok (UT) *Database Optimization Aspects for Information Retrieval*
04 Juan Roberto Castelo Valdueza (UU) *The Discrete Acyclic Digraph Markov Model in Data Mining*
05 Radu Serban (VU) *The Private Cyberspace Modeling Electronic Environments inhabited by Privacy-concerned Agents*
06 Laurens Mommers (UL) *Applied legal epistemology; Building a knowledge-based ontology of the legal domain*
07 Peter Boncz (CWI) *Monet: A Next-Generation DBMS Kernel For Query-Intensive Applications*
08 Jaap Gordijn (VU) *Value Based Requirements Engineering: Exploring Innovative E-Commerce Ideas*
09 Willem-Jan van den Heuvel (KUB) *Integrating Modern Business Applications with Objectified Legacy Systems*
10 Brian Sheppard (UM) *Towards Perfect Play of Scrabble*
11 Wouter C.A. Wijngaards (VU) *Agent Based Modelling of Dynamics: Biological and Organisational Applications*
12 Albrecht Schmidt (UvA) *Processing XML in Database Systems*
13 Hongjing Wu (TUE) *A Reference Architecture for Adaptive Hypermedia Applications*
14 Wieke de Vries (UU) *Agent Interaction: Abstract Approaches to Modelling, Programming and Verifying Multi-Agent Systems*
15 Rik Eshuis (UT) *Semantics and Verification of UML Activity Diagrams for Workflow Modelling*
16 Pieter van Langen (VU) *The Anatomy of Design: Foundations, Models and Applications*
17 Stefan Manegold (UvA)*Understanding, Modeling, and Improving Main-Memor Database Performance*

2003

01 Heiner Stuckenschmidt (VU) *Ontology-Based Information Sharing in Weakly Structured Environments*
02 Jan Broersen (VU) *Modal Action Logics for Reasoning About Reactive Systems*
03 Martijn Schuemie (TUD) *Human-Computer Interaction and Presence in Virtual Reality Exposure Therapy*
04 Milan Petkovic (UT) *Content-Based Video Retrieval Supported by Database Technology*
05 Jos Lehmann (UvA) *Causation in Artificial Intelligence and Law – A modelling approach*
06 Boris van Schooten (UT) *Development and specification of virtual environments*
07 Machiel Jansen (UvA) *Formal Explorations of Knowledge Intensive Tasks*
08 Yongping Ran (UM) *Repair Based Scheduling*
09 Rens Kortmann (UM) *The resolution of visually guided behaviour*
10 Andreas Lincke (UvT) *Electronic Business Negotiation: Some experimental studies on the interaction between medium, innovation context and culture*
11 Simon Keizer (UT) *Reasoning under Uncertainty in Natural Language Dialogue using Bayesian Networks*
12 Roeland Ordelman (UT) *Dutch speech recognition in multimedia information retrieval*
13 Jeroen Donkers (UM) *Nosce Hostem – Searching with Opponent Models*
14 Stijn Hoppenbrouwers (KUN) *Freezing Language: Conceptualisation Processes across ICT-Supported Organisations*
15 Mathijs de Weerdt (TUD) *Plan Merging in Multi-Agent Systems*

16 Menzo Windhouwer (CWI) *Feature Grammar Systems – Incremental Maintenance of Indexes to Digital Media Warehouses*
17 David Jansen (UT) *Extensions of Statecharts with Probability, Time, and Stochastic Timing*
18 Levente Kocsis (UM) *Learning Search Decisions*

2004

01 Virginia Dignum (UU) *A Model for Organizational Interaction: Based on Agents, Founded in Logic*
02 Lai Xu (UvT) *Monitoring Multi-party Contracts for E-business*
03 Perry Groot (VU) *A Theoretical and Empirical Analysis of Approximation in Symbolic Problem Solving*
04 Chris van Aart (UvA) *Organizational Principles for Multi-Agent Architectures*
05 Viara Popova (EUR) *Knowledge discovery and monotonicity*
06 Bart-Jan Hommes (TUD) *The Evaluation of Business Process Modeling Techniques*
07 Elise Boltjes (UM) *Voorbeeldig onderwijs; voorbeeldgestuurd onderwijs, een opstap naar abstract denken, vooral voor meisjes*
08 Joop Verbeek (UM) *Politie en de Nieuwe Internationale Informatiemarkt, Grensregionale politiele gegevensuitwisseling en digitale expertise*
09 Martin Caminada (VU) *For the Sake of the Argument; explorations into argument-based reasoning*
10 Suzanne Kabel (UvA) *Knowledge-rich indexing of learning-objects*
11 Michel Klein (VU) *Change Management for Distributed Ontologies*
12 The Duy Bui (UT) *Creating emotions and facial expressions for embodied agents*
13 Wojciech Jamroga (UT) *Using Multiple Models of Reality: On Agents who Know how to Play*
14 Paul Harrenstein (UU) *Logic in Conflict. Logical Explorations in Strategic Equilibrium*
15 Arno Knobbe (UU) *Multi-Relational Data Mining*
16 Federico Divina (VU) *Hybrid Genetic Relational Search for Inductive Learning*
17 Mark Winands (UM) *Informed Search in Complex Games*
18 Vania Bessa Machado (UvA) *Supporting the Construction of Qualitative Knowledge Models*
19 Thijs Westerveld (UT) *Using generative probabilistic models for multimedia retrieval*
20 Madelon Evers (Nyenrode) *Learning from Design: facilitating multidisciplinary design teams*

2005

01 Floor Verdenius (UVA) *Methodological Aspects of Designing Induction-Based Applications*
02 Erik van der Werf (UM) *AI techniques for the game of Go*
03 Franc Grootjen (RUN) *A Pragmatic Approach to the Conceptualisation of Language*
04 Nirvana Meratnia (UT) *Towards Database Support for Moving Object data*
05 Gabriel Infante-Lopez (UVA) *Two-Level Probabilistic Grammars for Natural Language Parsing*
06 Pieter Spronck (UM) *Adaptive Game AI*
07 Flavius Frasincar (TUE) *Hypermedia Presentation Generation for Semantic Web Information Systems*
08 Richard Vdovjak (TUE) *A Model-driven Approach for Building Distributed Ontology-based Web Applications*
09 Jeen Broekstra (VU) *Storage, Querying and Inferencing for Semantic Web Languages*
10 Anders Bouwer (UVA) *Explaining Behaviour: Using Qualitative Simulation in Interactive Learning Environments*
11 Elth Ogston (VU) *Agent Based Matchmaking and Clustering – A Decentralized Approach to Search*
12 Csaba Boer (EUR) *Distributed Simulation in Industry*
13 Fred Hamburg (UL) *Een Computermodel voor het Ondersteunen van Euthanasiebeslissingen*
14 Borys Omelayenko (VU) *Web-Service configuration on the Semantic Web; Exploring how semantics meets pragmatics*
15 Tibor Bosse (VU) *Analysis of the Dynamics of Cognitive Processes*
16 Joris Graaumans (UU) *Usability of XML Query Languages*
17 Boris Shishkov (TUD) *Software Specification Based on Re-usable Business Components*

18 Danielle Sent (UU) *Test-selection strategies for probabilistic networks*
19 Michel van Dartel (UM) *Situated Representation*
20 Cristina Coteanu (UL) *Cyber Consumer Law, State of the Art and Perspectives*
21 Wijnand Derks (UT) *Improving Concurrency and Recovery in Database Systems by Exploiting Application Semantics*

2006

01 Samuil Angelov (TUE) *Foundations of B2B Electronic Contracting*
02 Cristina Chisalita (VU) *Contextual issues in the design and use of information technology in organizations*
03 Noor Christoph (UVA) *The role of metacognitive skills in learning to solve problems*
04 Marta Sabou (VU) *Building Web Service Ontologies*
05 Cees Pierik (UU) *Validation Techniques for Object-Oriented Proof Outlines*
06 Ziv Baida (VU) *Software-aided Service Bundling – Intelligent Methods & Tools for Graphical Service Modeling*
07 Marko Smiljanic (UT) *XML schema matching – balancing efficiency and effectiveness by means of clustering*
08 Eelco Herder (UT) *Forward, Back and Home Again – Analyzing User Behavior on the Web*
09 Mohamed Wahdan (UM) *Automatic Formulation of the Auditor's Opinion*
10 Ronny Siebes (VU) *Semantic Routing in Peer-to-Peer Systems*
11 Joeri van Ruth (UT) *Flattening Queries over Nested Data Types*
12 Bert Bongers (VU) *Interactivation – Towards an e-cology of people, our technological environment, and the arts*
13 Henk-Jan Lebbink (UU) *Dialogue and Decision Games for Information Exchanging Agents*
14 Johan Hoorn (VU) *Software Requirements: Update, Upgrade, Redesign – towards a Theory of Requirements Change*
15 Rainer Malik (UU) *CONAN: Text Mining in the Biomedical Domain*
16 Carsten Riggelsen (UU) *Approximation Methods for Efficient Learning of Bayesian Network*
17 Stacey Nagata (UU) *User Assistance for Multitasking with Interruptions on a Mobile Device*
18 Valentin Zhizhkun (UVA) *Graph transformation for Natural Language Processing*
19 Birna van Riemsdijk (UU) *Cognitive Agent Programming: A Semantic Approach*
20 Marina Velikova (UvT) *Monotone models for prediction in data mining*
21 Bas van Gils (RUN) *Aptness on the Web*
22 Paul de Vrieze (RUN) *Fundaments of Adaptive Personalisation*
23 Ion Juvina (UU) *Development of Cognitive Model for Navigating on the Web*
24 Laura Hollink (VU) *Semantic Annotation for Retrieval of Visual Resources*
25 Madalina Drugan (UU) *Conditional log-likelihood MDL and Evolutionary MCMC*
26 Vojkan Mihajlovic (UT) *Score Region Algebra: A Flexible Framework for Structured Information Retrieval*
27 Stefano Bocconi (CWI) *Vox Populi: generating video documentaries from semantically annotated media repositories*
28 Borkur Sigurbjornsson (UVA) *Focused Information Access using XML Element Retrieval*

2007

01 Kees Leune (UvT) *Access Control and Service-Oriented Architectures*
02 Wouter Teepe (RUG) *Reconciling Information Exchange and Confidentiality: A Formal Approach*
03 Peter Mika (VU) *Social Networks and the Semantic Web*
04 Jurriaan van Diggelen (UU) *Achieving Semantic Interoperability in Multi-agent Systems: a dialogue-based approach*
05 Bart Willem Schermer (UL) *Software Agents, Surveillance, and the Right to Privacy: a Legislative Framework for Agent-enabled Surveillance*

In de boekenreeks van het E.M. Meijers Instituut voor Rechtswetenschappelijk Onderzoek van de Faculteit der Rechtsgeleerdheid, Universiteit Leiden, zijn in 2005 en 2006 verschenen:

MI-84 J.H. Crijns, P.P.J. van der Meij & G.K. Schoep (red.), *De taak van de strafrechtswetenschap,* Den Haag: Boom Juridische uitgevers 2005, ISBN 90 5454 554 2

MI-85 G.K. Schoep & P.M. Schuyt, *Instrumenten ter ondersteuning van de rechter bij straftoemeting,* Nijmegen: Wolf Legal Publishers 2005, ISBN 90 5850 107 8

MI-86 M.E. Koppenol-Laforce (red.), *De Europese vennootschap (SE) in de praktijk,* Deventer: Kluwer, ISBN 90 13023 22 3

MI-87 A.P.A. Broeders, *Ontwikkelingen in de criminalistiek. Van vingerspoor tot DNA-profiel B van zekerheid naar waarschijnlijkheid*, Den Haag: Boom Juridische uitgevers 2005, ISBN 90 5454 576 3

MI-88 I.S.J. Houben, *Contractdwang* (diss. Leiden), Deventer: Kluwer 2005, ISBN 90 1302 715 6

MI-89 T. Barkhuysen, W. den Ouden & J.E.M. Polak (red.), *Recht realiseren. Bijdragen rond het thema adequate naleving van rechtsregels,* Deventer: Kluwer 2005, ISBN 90 130 2811 X

MI-90a L. Reurich, *De articulatie van gedragsnormen. Deel I: normen van vaagheid,* Deventer: Kluwer 2005

MI-90b L. Reurich, *De articulatie van gedragsnormen. Deel II: vaagheid van normen* (diss. Leiden), Kluwer: Deventer 2005, ISBN 90 1302 776 8

MI-91 R. Haveman & H. Wiersinga, *Langs de randen van het strafrecht,* Nijmegen: Wolf Legal Publishers 2005, ISBN 90 5850 116 7

MI-92 P.C. van Es, *De actio negatoria. Een studie naar de rechtsvorderlijke zijde van het eigendomsrecht,* (diss. Leiden), Nijmegen: Wolf Legal Publishers 2005, ISBN 90 5850 131 0.

MI-93 R.W.M. Giard, *Aansprakelijkheid van artsen. Juridische theorie en medische praktijk*, Den Haag: Boom Juridische uitgevers 2005, ISBN 90 5454 633 6

MI-94 W. den Ouden (red.), *Staatssteun en de Nederlandse rechter,* Deventer: Kluwer 2005, ISBN 90 1303 063 7

MI-95 F. Hamburg, *Een computermodel voor het ondersteunen van euthanasiebeslissingen,* (diss. Leiden), Antwerpen: Maklu 2005, ISBN 90 4660 020 3

MI-96 J.P. Loof, *Mensenrechten en staatsveiligheid: verenigbare grootheden?*, (diss. Leiden), Nijmegen: Wolf Legal Productions 2005, ISBN 90 5850 147 7

MI-97 J.A.A. Adriaanse, *Restructuring in the shadow of the law. Informal reorganisation in the Netherlands*, (diss. Leiden), Deventer: Kluwer 2005, ISBN 90 1303 156 0

MI-98 A.O. Lubbers, M. Schuver-Bravenboer & H. Vording (red.), *Opstellen fiscaal overgangsbeleid*, Deventer: Kluwer 2005, ISBN 90 1303 212 5

MI-99 V. Van Den Eeckhout, C.J. Forder, E. Hooghiemstra, E. Nicolai & S.K. van Walsum, *Transnationale gezinnen in Nederland*, Den Haag: Boom Juridische uitgevers 2005, ISBN 90 5454 652 2

MI-100 J.H. Nieuwenhuis & C.J.J.M. Stolker (red.), *Vooruit met het recht. Wat geldt in de rechtswetenschap als vooruitgang?*, Den Haag: Boom Juridische uitgevers 2006, ISBN 90 5454 741 3

MI-101 G.C. Coteanu, *Cyber Consumer Law. State of the Art and Perspectives*, (diss. Leiden) 2005, Roemenië: Humanitas 2005, ISBN 973 50 1106 9

MI-102 BWKJ-21: E.M. Hoogervorst, I.S.J. Houben, P. Memelink, J.H. Nieuwenhuis, L. Reurich & G.J.M. Verburg, *Rechtseenheid en vermogensrecht*, Deventer: Kluwer 2005, ISBN 90 1303 097 1

MI-103 A. Tsoutsanis, *Het merkdepot te kwader trouw*, (diss. Leiden), Deventer: Kluwer 2005, ISBN 90 13 03252 4

MI-104 E.C.C. Punselie, *Voor een pleegkind met recht een toekomst*, (diss. Leiden), Deventer: Kluwer 2006, ISBN 90 13 03328 8

MI-105 A. Hendriks, *In beginsel. De gezondheidsrechtelijke beginselen uitgediept,* (oratie Leiden), Leiden: NJCM-boekerij 2006, ISBN 90 6750 046 1

MI-106 T. Barkhuysen, *Eenheid en coherentie van rechtsbescherming in de veellagige Europese rechtsorde,* (oratie Leiden), Deventer: Kluwer 2006, ISBN 90 1303 568 X

MI-107 N.J.H. Huls & Z.D. Laclé, *Meer macht voor de consument?*, Deventer: Kluwer 2006, ISBN 90 5454 697 2

MI-108 W. Zwalve, *Simplex et perpetuum. Beschouwingen over eigendom en tijd,* Den Haag: Boom Juridische uitgevers 2006, ISBN 90 54547 12 X

MI-109 T.J. de Graaf, *Exoneraties in (ICT-)contracten tussen professionele partijen,* Deventer: Kluwer 2006, ISBN 90 1303 660 0

MI-110 N. Jungmann, *De Wsnp: bedoelde en onbedoelde effecten op het minnelijk traject*, Leiden: Leiden University Press 2006, ISBN 90 8728 004 1

MI-111 R. van Alebeek, *The Immunity of States and their Officials in the Light of International Criminal Law and International Human Rights Law*, (diss. Leiden) 2006

MI-112 J.H. Gerards, *Belangenafweging bij rechterlijke toetsing aan fundamentele rechten*, (oratie Leiden), Deventer: Kluwer 2006, ISBN 90 13 03837 9

MI-113 W. Huisman, M. Moerings en G. Suurmond (red.), *Veiligheid en recht: nieuwe doelwitten en nieuwe strategieën*, Boom Juridische uitgevers 2006, ISBN 90 5454 732 4

MI-114 A.C. Rijkers & H. Vording (red.), *Vijf jaar Wet IB 2001*, Deventer: Kluwer 2006, ISBN 90 13 03851 4

MI-115 T. Barkhuysen, W. den Ouden & Y.E. Schuurmans (red.), *Het model Tak: Verhoogde rechtsbescherming in het bestuursrecht?*, Alphen aan den Rijn: Kluwer 2006, ISBN 90 1303 852 2

MI-116 Y.E. Schuurmans (red.), *Bewijzen en beslissen*, Deventer: Kluwer 2006, ISBN 90 1303 756 9

MI-117 H.J.Th.M. van Roosmalen, *Overheidsaansprakelijkheid in Engeland en Nederland*, (diss. Leiden), Den Haag: Sdu 2007, ISBN 978 90 12 11846 0

MI-118 R.W.J. Crommelin, *Het aanvullen van de rechtsgronden*, (diss. Leiden), Alphen aan den Rijn: Kluwer 2007, ISBN 978 90 1304635 9

MI-119 L.A.R. Siemerink, *De overeenkomst van Internet Service Providers met consumenten*, (diss. Leiden), Deventer: Kluwer 2007, ISBN 90 13 04357 7

MI-120 I.S.J. Houben, K.J.O. Jansen, P. Memelink, J.H. Nieuwenhuis & L. Reurich (red.), *Europees contractenrecht. Techniek en moraal*, Deventer: Kluwer 2007, ISBN 90 13 04036 5

MI-121 S. Hillebrink, *Political Decolonization and Self-Determination. The Case of the Netherlands Antilles and Aruba*, (diss. Leiden) 2007, ISBN 978 90 9021470 2

MI-122 B.W. Schermer, *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance*, (diss. Leiden) Leiden: Leiden University Press 2007, ISBN 978 90 8728 021 5

Zie voor de volledige lijst van publicaties: www.law.leidenuniv.nl/onderzoek